УДК 007:004.56:341.174(4)

В. Д. Бойко, М. Д. Василенко

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ЄС: ПРОБЛЕМИ ЦИФРОВОГО СУСПІЛЬСТВА

Постановка проблеми. Реалії інформаційної безпеки та кібербезпеки, технологічний прогрес та активність цифрового суспільства у мережі зумовлюють те, що наразі сучасні суспільні відносини характеризуються широким використанням персональних даних під час обігу інформації, товарів, послуг і капіталів, що вимагає не тільки вільного руху інформації про особу, а й забезпечення її надійного захисту відповідно до основних прав і свобод людини. Одним з найважливіших проблемних питань у сфері Інтернету речей сьогодні є питання захисту персональних даних. Враховуючи рівень інформатизації та розвитку технологій, в ЄС використовують такий термін, як приватність (privacy), яка для багатьох людей вбачається правовою категорією, що потребує додаткового захисту. В такій ситуації очевидно, що захист персональних даних фізичних осіб та можливість реального впливу фізичних осіб (суб'єктів персональних даних) на умови їх обробки в мережі Інтернет в сучасних умовах стають вельми актуальними, особливо в умовах розвитку таких технологій, як «великі дані» та «Інтернет речей». Слушно зауважити, що захист фізичних осіб під час опрацювання персональних даних є фундаментальним правом, адже згідно зі статтею 8 (1) Хартії Європейського Союзу про основні права та статтею 16 (1) Договору про функціонування Європейського Союзу кожна особа має право на захист своїх персональних даних. Водночас прогрес у галузі інформаційних технологій, зокрема, у сфері розробки та впровадження програмного забезпечення, активність у формуванні баз персональних даних надзвичайно загострили проблему захисту приватного життя фізичних осіб.

Слід зазначити, що деякі питання формування та правового регулювання системи захисту персональних даних ЄС відмічені у наукових доробках таких вітчизняних і зарубіжних вчених, як Л. Брендайс, В.М. Брижко, М. Бунда, С. Ворен, В.А. Копилов, К. Кунер, М. Лаббок, А. Марошч, П.Г. Мехіа, В.І. Муравйов, А.В. Пазюк, А.І. Радянська, Н. Флірі, Г.Г. Фустер, Т. Хікман, О.О. Шевчук, М.Я. Швець. Однак проблемні аспекти захисту

персональних даних в Європейському Союзі через призму кібербезпеки та цифрового суспільства досі не було розглянуто, що й зумовлює актуальність і теоретико-практичний інтерес до обраної теми дослідження.

Метою статті є дослідження захисту персональних даних в ЄС як реалії цифрового суспільства та вирішення проблемних питань з позицій кібербезпеки.

Виклад основного матеріалу. Глобалізація та технологічний прогрес створили багато різних проблем під час реалізації фізичними особами свого права на захист персональних даних, з якими зіткнулися і в країнах-членах та в самому ЄС в цілому. Персональні дані завдяки сучасним технологіям переміщаються вільніше, приватні компанії та органи державної влади використовують персональні дані в небувалих раніше масштабах, фізичні особи все більше і більше відкривають доступ до своїх даних. Захист персональних даних також є невіддільною частиною правового регулювання в рамках інформаційного суспільства.

Зробимо невеликий історичний екскурс щодо питання персональних даних в ЄС, а потім обговоримо законодавство ЄС щодо захисту персональних даних, яке набуло чинності з 25 травня 2018 р.

Перші рекомендації в Співтоваристві (1980 р.) не мали обов'язкового характеру для країн-членів, тому не було єдиного орієнтира для всіх країн-членів. Відповідно, національне законодавство дуже відрізнялося та було різноманітним. Відмінності негативно впливали на внутрішній ринок, через що було ініційовано прийняття у 1995 р. Директиви 45/46/ЄС як єдиного обов'язкового акту для всіх країн-членів. Однак у ній не було враховано майбутній технологічний прогрес, тому незабаром виникло питання про розробку нового більш прогресивного акту. Отже, у січні 2012 року було ініційовано реформування законодавства ЄС у сфері захисту персональних даних з метою приведення його у відповідність до вимог «цифрової епохи» та на виконання Стратегії єдиного цифрового ринку Європи (Digital Single Market Strategy). У зв'язку з цим було розроблено та впроваджено два документи. Перший – Директива 2016/680 Європейського Парламенту та Ради ЄС від 27 квітня 2016 р. «Про захист фізичних осіб щодо обробки персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування кримінальних злочинів або виконання кримінальних покарань та про вільне переміщення таких даних, а також про скасування Рамкового Рішення Ради 2008/977» [1]; другий – Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року (General Data Protection Regulation (GDPR), Загальний регламент про захист даних) «Про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС» [2]. Директива набула чинності 24 травня 2016 року, але країни-члени мали транспонувати її в своє національне законодавство до 6 травня 2018 року. Регламент як нормативно-правовий акт прямої дії автоматично став частиною національного законодавства кожної країни-члена з 25 травня 2018 року.

Зазначимо, що положення Регламенту спрямовані на гармонізацію захисту основних прав і свобод фізичних осіб щодо діяльності з переробки і на забезпечення вільного потоку персональних даних між державами-членами. Єдиний для всіх країн-членів Регламент має сприяти розбудові простору свободи, безпеки, справедливості й економічного союзу; економічного і соціального прогресу; зміцненню законності і зближенню економік в рамках внутрішнього ринку, а також загальному добробуту фізичних осіб країн-членів. Директива більш детально визначає умови співпраці з правоохоронними органами.

Головні новації, які внесені в право ЄС цими документами можна сформулювати наступним чином. Регламент вводить такі поняття, як «контролер» (самостійно або спільно з іншими визначає цілі та засоби опрацювання персональних даних) та «оператор» (опрацьовує персональні дані від імені контролера). Крім того, було розширено поняття «персональні дані» через те, що фізичні особи можуть бути пов'язані з онлайн-ідентифікаторами за допомогою їхніх пристроїв, додатків, інструментів чи протоколів, зокрема, IP-адресу, ідентифікаторів «cookie» (реп'яшків) або інших ідентифікаторів, таких як мітки радіочастотної ідентифікації. Це може залишити підказки, які в поєднанні з унікальними ідентифікаторами та іншою інформацією, отриманою з серверів, можна використати для створення профілів фізичних осіб та їхньої ідентифікації. Тепер згода на зберігання персональних даних, відображена у письмовому чи електронному вигляді, на вимогу контролюючих органів має бути пред'явлена. Введено право «право бути забутим» (право вимагати знищення усіх персональних даних після закінчення терміну їх обробки). Зазначимо, що це право не стало новим через те, що воно вперше було зазначене у рішенні Суду ЄС у справі «Google Spain» від 14 травня 2014 р. [3], у якому Суд ЄС на прецедентному рівні визнав за суб'єктом персональних даних «право бути забутим» (right to be forgotten) в ролі невіддільного права людини. Крім того, важливо зауважити, що це право не є абсолютним, адже його реалізація можлива лише за дотримання певних умов, наприклад, данні більше не потрібні компанії для тієї мети, задля якої вони були зібрані, або основою обробки даних є не згода фізичної особи, а вимога законодавства. В зв'язку з цим можна навести практичний приклад реалізації цього права: звільнений працівник вимагає у роботодавця знищити всі дані про нього, а роботодавець знає, що знищивши ці дані, він порушить законодавчі вимоги щодо строків зберігання трудових документів. У зв'язку з цим виникає питання, як співвідносити «право бути забутим» і обов'язок зберігання документів. Через те, що обробка даних (зберігання) здійснюється на основі вимог законодавства, а не на основі згоди суб'єкта, «право бути забутим» не застосовується. Важливим аргументом проти права бути забутим є твердження про те, що пошукові системи в Інтернеті не можна вважати контролерами даних у розумінні законодавства ЄС [4, с. 775]. Саме така ідея обґрунтована у позиції Генерального адвоката по справі «Маріо Констехи Гонсалеса». Зокрема, він вважає, що пошукова система в Інтернеті у процесі пошуку

не продукує новий автономний контент, виконує функції лише передавання даних, а її оператор не може нести обов'язків, які покладають на контролера даних [5]. Отже, у такому випадку (а також у випадку, якщо усе ж розглядати оператора пошукової системи як контролера даних), суб'єкту даних, який вважає, що його права чи інтереси порушені, доцільніше звертатися безпосередньо до сайтів-першоджерел, тобто до тих, хто розмістив інформацію в Інтернеті, а не до пошукової системи. Стосовно цього важливо правильно оцінювати і чітко розмежовувати діяльність, обов'язки та відповідальність кожного суб'єкта. Зокрема, коли йдеться про суб'єкта, який оприлюднює інформацію та є впливовим у медіа-просторі (як-от ЗМІ), то у відносинах з ним права людини захищені за допомогою низки правових інститутів. Наприклад, за допомогою права на відповідь зацікавлена особа може оприлюднити власну позицію такої ж ваги, як і оскаржувана інформація. Своєю чергою великі пошукові системи є надзвичайно впливовими суб'єктами відносин в Інтернеті, а «контент», який вони продукують, – це підбір та порядок посилань у відповідь на запит [6, с. 769]. Неважко уявити ситуацію, коли звернення до сайту-першоджерела не вирішить проблеми. Наприклад, відповідь чи спростування опублікованої сайтом недостовірної інформації на своїй головній сторінці зовсім не гарантує, що ця відповідь буде на першій, а не на сотій сторінці результатів, які видає пошукова система.

Отже, необхідні спеціальні правові норми, які захищатимуть користувача Інтернету у різних обставинах, і саме закріплення можливості вимагати стирання інформації про себе у праві ЄС є результатом намагань створити такі норми. З іншого боку, логічно виділити захист володільцями персональних даних «за конструкцією» (by design) та «за замовченням» (by default). Фактично вони мають принциповий характер. Перше визначення означає, що володілець персональних даних як під час проголошення мети обробки, так і в процесі самої обробки має гарантувати відповідність усієї процедури Регламенту. Друге визначення має забезпечити те, що володілець має імплементувати механізми гарантування того, що за замовченням обробляються лише ті персональні дані, які є необхідними для кожної детально визначеної мети обробки, і не зберігаються поза межами мінімальних строків, необхідних для досягнення таких цілей. Ці механізми повинні також забезпечити, щоб персональні дані не були доступними невизначеному колу осіб. Із зазначеного вище випливають принципи Privacy by Design, серед яких основними виступають ті, що є нижчезазначеними [7].

1) Використання превентивних заходів, а не тільки усунення наслідків: вбудовування конфіденційності в конструкцію системи повинне бути активним, а не обмежуватися лише заходами по усуненню наслідків. Такий підхід передбачає і запобігає випадкам порушення конфіденційності ще до того, як вони відбуваються. Іншими словами, особиста інформація повинна бути захищена до того, як система запущена в роботу, а не після виявлення порушень конфіденційності.

2) Визначення умов конфіденційності як стандартної установки: Privacy by Design прагне досягти максимального ступеня захисту особистої інформації, гарантуючи, що персональні дані захищені автоматично в тій або іншій інформаційній системі або ділових відносинах. Навіть якщо індивідуум не вживає ніяких заходів, його особиста інформація залишається надійно захищеною. Не вимагається ніяких дій з боку індивідуума для захисту особистої інформації, – система вже спочатку містить в собі необхідні установки.

3) Конфіденційність виступає як частина структури: захист особистої інформації повинен стати невіддільною частиною архітектури будь-якої інформаційної системи або ділових відносин. Це не якийсь додатковий компонент, внесений в систему постфактум.

4) Реалізація повної функціональності із сумарним позитивним результатом: Privacy by Design не шукає приводів для помилкової дихотомії, таких, наприклад, як зміцнення безпеки системи на противагу захисту особистої інформації, демонструючи, що можна забезпечити, тощо.

5) Захист особистої інформації впродовж всього циклу її збору, зберігання, обробки і знищення: конфіденційність повинна бути вбудована в систему ще до початку збору даних. Навіть більше, цей захист повинен надійно розповсюджуватися на весь цикл зберігання і обробки даних; іншими словами, збереження даних має важливе значення для конфіденційності від моменту запуску системи і до кінця її існування. Це гарантує надійне зберігання даних, а після закінчення їх використовування – надійне і своєчасне знищення.

6) Реалізація доступності та відвертості: всі компоненти і операції залишаються відкритими і доступними як для користувачів, так і для тих, хто забезпечує даний вид сервісу.

7) Реалізація дотримання конфіденційності користувачів: система повинна бути орієнтована на користувача. Це досягається такими заходами, як захист особистої інформації за умовчанням, своєчасне повідомлення про збір особистої інформації, надання користувачу свободи вибору в зручній і зрозумілій формі.

Як відомо, сьогодні ЄС не має своїх власних пошукових систем, соціальних мереж тощо, тому він має йти в фарватері США, захищаючи свої власні інтереси. Так, наприклад, питання передачі персональних даних третій країні або міжнародній організації може мати місце лише за умови, якщо передача даних необхідна: для захисту життєво важливих інтересів суб'єкта даних або іншої особи; для захисту законних інтересів суб'єкта даних, якщо це передбачено законодавством держави-члена стосовно передачі персональних даних; для запобігання прямій і серйозній загрозі для громадської безпеки держави-члена або третьої країни. Право знати про злами баз персональних даних (компанії та організації мають повідомляти свої національні контролюючи органи про будь-які загрози для персональних даних суб'єктів цих даних, а також вступати в комунікації з самим суб'єктами даних щодо цих ризиків). Має бути легший доступ

до своїх даних, тоді фізичні особи будуть мати більше інформації про те, яким чином обробляється їх персональні дані, яка саме інформація є у компанії, з якою метою вона зберігається, яким третім особам передається, як довго зберігатимуться персональні дані і яке джерело збору інформації. Ця інформація має бути надана чітко та зрозуміло і винятково на безоплатній умові. При цьому існує право на переніс персональних даних (right of data portability): фізичні особи зможуть переносити свої персональні дані при зміні провайдерів послуг. Отже, натепер встановлена більш жорстка відповідальність за порушення вимог до захисту персональних даних. Законодавчо реалізується необхідність призначати окремих фахівців (штатних або найманих за контрактом) або створювати окремі підрозділи для обробки персональних даних. Природно, що при згаданій залежності від провідних комп'ютерних компаній США, що є власниками Інтернету, пошукових, інших систем тощо, вплив на збереження персональних даних відбувається через систему штрафів. Так, штраф в розмірі 10 мільйонів Євро або 2 відсотків річного обігу (в залежності від того, що вище) буде стягнуто за порушення наступних положень Регламенту [2]: ст. 8 (щодо умов отримання згоди неповнолітніх), ст. 11 (щодо обробки, яка не потребує ідентифікації), ст. 25-39 (що стосуються володільця та розпорядника, безпеки персональних даних, оцінки впливу обробки персональних даних та попередні консультації, призначення відповідального за безпеку персональних даних), ст. 41 (4) обов'язки органу моніторингу), ст. 42 (правила сертифікації) та ст.43 (органи сертифікації).

Штрафом в розмірі 20 мільйонів Євро або 4 відсотків річного обігу (в залежності від того, що вище) буде каратись порушення положень Регламенту, що стосуються:

а) основних принципів обробки персональних даних, в першу чергу згоди (ст. 5), легітимності обробки (ст. 6), умов отримання згоди (ст. 7), обробки особливих категорій персональних даних (ст. 9);

б) прав суб'єкта даних, що визначені (ст. 12-22);

в) правил трансферу персональних даних в треті країни або міжнародним організаціям (ст. 44-49);

г) положень щодо специфічних ситуацій обробки (Глава IX);

д) невиконання наказів чи вимоги контролюючого органу щодо обмеження обробки або припинення переміщення даних (ст. 58 (2)) або ненадання доступу (ст. 58 (1)).

В рамках GDPR, «робоча група 29» (working party 29) надає роз'яснення та Керівні принципи (guidance) з різних питань, що виникають у контролерів та процесорів (як вони визначені в рамках GDPR) щодо різних аспектів застосування вказаного Регламенту. Одне з таких роз'яснень стосується «прозорості» під час обробки персональних даних (далі Керівні принципи) [8].

Як вказано у самих Керівних принципах, «прозорість» є всеосяжним обов'язком для контролерів та операторів (як вони визначені GDPR) та застосовується у наступних трьох ключових сферах: 1) надання інформації

суб'єктам персональних даних для чесної обробки; 2) умови комунікації контролерів з суб'єктами персональних даних щодо їхніх прав в рамках GDPR; 3) забезпечення реалізації прав суб'єктів персональних даних контролерами [8].

В Керівних принципах наводяться приклади правильної та слабкої (невдалої) комунікації обробників з суб'єктами персональних даних в контексті «прозорості», зокрема, наводяться такі вирази: 1) «ми можемо використовувати Ваші персональні дані для розвитку нових сервісів»; 2) «ми можемо використовувати Ваші персональні дані для дослідницьких цілей»; 3) «ми можемо використовувати Ваші персональні дані для пропонування персоналізованих сервісів». Всі вищевказані способи комунікації названі прикладами слабкої/невірної практики (poor practice example). Причиною цьому служить «загальність» висловлювань – не вказано, які саме сервіси будуть розвиватись, та як саме в цьому разі будуть використовуватись персональні дані, не вказано, яке саме дослідження відбудеться та які саме сервіси планується надавати в майбутньому.

Комунікація з суб'єктом персональних даних може також доповнюватись візуальними об'єктами для кращого та всебічного сприйняття таким суб'єктом інформації. Така умова передбачена статтею 12 GDPR. Ще однією умов прозорості, як це вказано у Керівних принципах, є використання простої мови, яка буде зрозуміла потенційній цільовій аудиторії. Таким чином, в рамках GDPR термін «прозорість» під час обробки персональних даних означає реальну можливість для суб'єктів персональних даних розуміти, що і як відбувається з їх персональними даними.

На наш погляд, також слід детальніше звернути увагу на положення Директиви (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.2016 р. «Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і важкого злочину» (Директива PNR) [9], оскільки вона входила у законодавчий пакет ЄС із захисту персональних даних.

Зібрані дані PNR можуть бути оброблені тільки для профілактики, виявлення, розслідування і судового переслідування терористичних і серйозних злочинів. Вони включають: ім'я пасажира, дату поїздки, маршрут проходження, відомості про квитки, контактні дані з турагентом, через якого політ був замовлений, використовувані засоби платежу, номер місця, відомості про багаж.

Нові правила визначають стандарт ЄС для обробки і використання даних PNR та включають положення, що належать до:

– мети, з якою дані PNR будуть оброблені в контексті правоохоронної діяльності (використання в розслідуваннях і судових переслідуваннях конкретних осіб);

– зберігання даних PNR (протягом 4,5 років), із суворою процедурою доступу до повної інформації (перелік даних, які збираються авіаперевізниками, представлений в Додатку 1 до Директиви PNR);

– обміну даними PNR між державами – членами ЄС та між державами – членами ЄС і третіми країнами. Обмін даними здійснюється за допомогою мереж обміну (електронних засобів), за умов забезпечення їх сумісності для форматів даних PNR і відповідних протоколів.

Забезпечення створення однакових умов сумісності, застосовних до передачі (електронної передачі) даних від авіаперевізників, покладено на Комісію ЄС. Ці повноваження мають здійснюватися відповідно до Регламенту (ЄС) № 182/2011 Європейського парламенту і Ради «Про правила і загальні принципи механізму контролю державами – членами ЄС та здійснення Комісією ЄС виконавчих повноважень». Розглядаючи зазначений документ, автори цієї статті (В.Б. та М.В.) звертають увагу на такі положення документу, як:

– посилення гарантій захисту приватного життя та персональних даних, зокрема, шляхом підвищення ролі національних наглядових органів і обов'язкового призначення співробітника по захисту даних PNR у відповідних організаціях;

– визначення в кожній державі – члені ЄС компетентного органу для профілактики, виявлення, розслідування або судового переслідування терористичних і серйозних злочинів для забезпечення виконання положень Директиви PNR. Національний контролюючий орган (Національний орган нагляду) кожної країни-члена відповідає за консультування і моніторинг застосування на своїй території прийнятих національних нормативних положень, згідно з Директивою PNR;

– призначення в кожному органі реєстрації авіапасажирів (ОРА) співробітника по захисту даних, відповідального за контроль обробки даних PNR і реалізацію правових гарантій. ОРА зобов'язаний вести облік наступних операцій обробки: збір, консультації, розкриття інформації та її стирання. Протоколи консультацій і розкриття інформації повинні містити, зокрема, мету, дату і час проведення таких операцій і вказувати, за можливістю, відомості про особу людини, яка консультувалася. Записи мають бути використані винятково для цілей перевірки, самоконтролю, забезпечення цілісності і безпеки даних або аудиту. ОРА повинен надавати записи по запиту Національного наглядового органу;

– встановлення правил відносно санкцій, зокрема фінансових, до авіаперевізників, які не передають дані.

В усіх відповідних документах ЄС вказується, що реформа системи правового регулювання захисту персональних даних має безпосереднє відношення до врегулювання питань кіберзахисту та забезпечення мережевої та інформаційної безпеки. Саме тому ці питання не можна розглядати окремо одне від одного. Водночас не можна не відзначити, що введення Регламенту ЄС [2] вносить певні серйозні обмеження. Так, можна зазначити, що GDPR приводить до неможливості використання в бізнесі рекламних і трекінгових додатків «третьої сторони». Дотримання GDPR приводить до ускладнення бізнес-аналітики сервісів і неможливості одержувати дохід від рекламних систем.

Згідно з [10] можна виділити наступні категорії користувачів сайтів бізнесу:

– одноразові відвідувачі;

– відвідувачі, що використовують сервіс частково (тимчасові користувачі);

– повноправні зареєстровані користувачі, що використовують велику частину функціональності сервісу;

– користувачі, що припинили використання сервісу (що автоматично має на увазі скасування реєстрації користувача і видалення з сервісу його персональних даних).

Для першої категорії можлива тільки «анонімна» аналітика, в якій поведінка користувача ніяк не пов'язана з його профілем або з його профілізацією – отриманням про нього будь-яких додаткових даних деанонімізуються.

Інша категорія представляє собою користувачів, які користуються функціоналом сервісу, але не всім, а тільки його частиною (наприклад, такі користувачі можуть бути підписані на оновлення або на новинні розсилки, але не зареєстровані як повноформатні користувачі сайту). Тут може бути одержана згода на використання даних користувача, але тільки часткове. Використання частки роботи реклами та аналітики бізнесу суворо обмежується цільовою установкою, що визначає частку інтересу користувача сервісу. Нарешті, для останньої категорії (повноправних користувачів сайту) стара модель використання реклами і аналітики бізнесу може бути задіяна повною мірою, проте все одно вимагає явної згоди користувача і не може бути використана без його відома.

GDPR так само змінює структуру роботи з даними користувачів тих, що відмовилися від використання сервісу. Якщо раніше інформація про таких користувачів могла залишатися в системі та використовуватися у всіх перерахованих вище випадках (реклама/маркетинг/таргетінг/бизнес-аналітика), то тепер такі дані повинні видалятися, а тому не можуть бути використані. Один із шляхів їх часткового використання – механізм «анонімізації», подібний тому, який використовується для першої категорії користувачів. При цьому дані про поведінку користувача відділяються від профілю користувача й можуть залишатися в системі навіть після стирання профілю користувача. Це дозволяє зберегти інформацію про взаємодії з користувачами сервісу, хоч і в неповному обсязі.

Впровадження суворих нормативів контролю за приватністю інформації про користувачів також потенційно може позначитися на якості сервісів, що надаються користувачам. Наприклад, дані про зростання, вагу, розмір взуття й інші біометричні параметри користувача є приватними, тому багато сервісів перестали дозволяти використовувати їх (наприклад, для розрахунку розмірів одягу, спортивного інвентарю тощо) без повної реєстрації. Так само повідомляється про відхід частини гральних сервісів з європейських ринків, оскільки вони теж зберігають призначені для користувача дані та потрапляють під дію GDPR. Крім загальних проблем,

пов'язаних з ускладненням бізнесу, позначається загальна неготовність гравців до нововведень. Наприклад, дослідження, проведене Ponemon Institute [11], показує загальну неготовність компаній до впровадження положень GDPR. Зокрема, крім загального поганого знайомства з положеннями GDPR, компанії виявляються не готовими до його реалізації. Так, встановлено [11]:

– у більш ніж двох третинах опитаних компаній не дотримуються терміни і вимоги обов'язкового сповіщення про витоки даних, що відбулися;

– більш ніж половина компаній вважає, що головною загрозою витоків може бути фінансовий збиток від штрафу згідно з вимогами GDPR;

– близько 60% компаній вважає, що впровадження GDPR приведе до необхідності серйозної реструктуризації компанії;

– найбільш важкою вимогою для компаній стає вимога про сповіщення про витоки даних і забезпечення користувачам доступу до їх даних (так вважають не менше 83% респондентів).

Також згідно з опитуванням, як свідчать ті ж самі матеріали, окрім реструктуризації компанії, більш ніж у половині випадків потрібним стає залучення окремих експертів з впровадження GDPR та інші аутсорсінгові заходи. В цілому дослідження [11] показує слабку готовність до реалізації положень GDPR серед широкого спектру компаній, оскільки в опитуванні брали участь компанії як з ЄС, так й із США.

Проблеми стосуються не тільки пересічних компаній, але й великих гравців ринку, які володіють всіма необхідними ресурсами для реструктуризації, але все одно не встигли провести реалізацію положень GDPR.

Згідно з дослідженням юриста і активіста в питаннях приватності Макса Шремса (Max Schrems), крупні гравці інформаційного ринку (зокрема, соціальні мережі, сервіси відеохостінгу та стрімінгового віщання) систематично порушують GDPR, що за різними оцінками у відповідь тільки на 10 основних скарг може обійтися крупним компаніям приблизно в 18,8 млрд євро штрафу [12]. Автор зазначає, що в багатьох компаніях реакція на скарги відбувається без участі людини – на базі тих або інших варіацій автовідповідачів і систем автоматичної відповіді на листи зі скаргами. У деяких компаніях користувачу надаються не всі дані або надаються дані, але не надається інформація про те, для чого й навіщо вони були використані та які треті сторони мали або могли мати до них доступ. При цьому такі компанії, як британський сервіс спортивного стрімінга DAZN і німецький музичний стрімінговий сервіс SoundCloud взагалі ігнорують запити про порушення GDPR.

Впровадження GDPR ставить під загрозу знищення цілого сегменту Інтернету, причому що належить до самих передових Інтернет-технологій [13]. Йдеться про розподілені системи, окремим прикладом яких є криптовалюти та блокчейн-технології.

У «розподіленому Інтернеті» дані зберігаються у вигляді окремих фрагментів інформації на кожному комп'ютері призначеної для користувача мережі. При цьому часто така мережа захищена особливими криптографічними

системами, які роблять неможливим управління даними, що зберігаються в інформаційному просторі такої мережі поза призначеною для користувача «точкою входу». Наприклад, в мережах **TOR** та **i2p** призначений для користувача трафік в закодованому вигляді проходить через всі мережеві крапки, розподіляючись між ними у випадковому порядку. Це приводить до фундаментальних суперечностей з GDPR [14]. Наприклад, в сучасному вигляді з таких мереж неможливо видалити призначені для користувача дані, не порушивши цілісність системи. Неможливо визначити, на якому комп'ютері територіально зберігаються дані користувача в різні моменти часу. Крім того, системи, засновані на блокчейн-технологіях, звичайно націлені на збереження історії дій користувача (інформація про операції по купівлі-продажу криптовалюти, смарт-контракти тощо), видалити які без порушення цілісності системи так само не уявляється можливим.

Хоча питання активно дискутується і вже запропоновані деякі шляхи рішення проблеми (наприклад, залишати тільки хэш-суми транзакцій після видалення даних [15]), тема співіснування розподілених мереж, заснованих на блокчейн-технологіях і GDPR, все ще залишається під питанням [16].

Всі перераховані проблеми говорять про те, що як самі положення GDPR, так і практика їх впровадження вимагають істотного доопрацювання [17]. В цьому відношенні певний інтерес можуть представляти міркування, які були висловлені на слуханнях сенатського комітету у юридичних справах США [18]. У числі запрошених на слухання виступили представники DuckDuckGo і Mapbox – фірм, що широко використовують відкритий, прозорий і відповідальний підхід до використання призначених для користувача даних, при цьому комерційно успішних фірм. Міркування, приведені представниками згаданих вище фірм, можна звести до трьох наступних пунктів щодо поліпшення загального контролю приватності, які цілком можна розповсюдити, зокрема, на практику рішення проблем з GDPR.

1) Дотримання приватності може бути корисним для бізнесу. Все залежить від вибраної моделі бізнесу, приклади DuckDuckGo, Mapbox і інших Інтернет-компаній показують, що цілком можна поєднувати отримання прибутку з відповідальним підходом до поводження з призначеними для користувача даними.

2) Контроль за приватністю не повинен ускладнювати ведення бізнесу. Це передусім стосується законодавчої бази. Зокрема, багато положень GDPR є суперечливими та вимагають подальшого роз'яснення. На противагу цьому, нове законодавство повинне забезпечувати максимально зрозумілий та доступний підхід до управління призначеними для користувача даними і чітко визначати відповідальність приватних компаній.

3) Впровадження законів повинне покладатися на самоорганізацію «нетізенів» (груп користувачів Інтернету та активістів, що само організовуються), а не на ініціативи «великих гравців», оскільки останні завжди діятимуть на користь бізнесу, а не Інтернет-співтовариства в цілому [19].

У сучасному інформаційному просторі існує велика кількість проблем, пов'язаних з приватністю та управлінням призначеними для користувача

даними. Для вирішення цього питання пропонуються різні шляхи. Нам представляється перспективним дотримання перерахованих заходів, яке повинне допомогти поліпшити положення справ як для рядових користувачів, так і для крупних гравців інформаційного ринку.

Висновки. Базовою метою захисту персональних даних стало забезпечення ключових прав та свобод громадян. Сьогодні основою захисту персональних даних в ЄС став пакет документів, базовим серед яких постає Регламент (ЄС) 2016/679 Європейського Парламенту та Ради (General Data Protection Regulation (GDPR), загальний регламент про захист даних), що регулює діяльність з переробки та забезпечення вільного потоку персональних даних між державами-членами. Незважаючи на гучні скандали щодо доступу та оприлюднення персональних даних та зростання критики на адресу соціальних мереж, у щоденному житті користувачі продовжують залишати чимало особистих даних (і не лише в мережі Інтернет), іноді навіть не здогадуючись про можливість використання їх третіми особами. Основною дилемою упорядкування інформаційних відносин у сфері захисту персональних даних залишається протиріччя між прагненням максимального застосування персональних даних у державних (міждержавних), політичних, комерційних та особистих інтересах й одночасно спрямованість у бажаннях та деклараціях захистити права на недоторканність приватного життя людини. Хоча ідея захисту персональних даних виходить з необхідності захисту індивідуума та гарантій верховенства його інтересів над «суспільними інтересами», деякі інтереси можуть виконувати волю однієї особи (чи групи) із силою та невідворотністю натовпу.

Література

1. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. URL: https://clck.ru/FEMNQ.

2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). URL: https://clck.ru/FEMPB.

3. Case C-131/12: Judgment of the Court (Grand Chamber) of 13 May 2014 (request for a preliminary ruling from the Audiencia Nacional – Spain) – Google Spain SL, Google Inc. v Agencia Espacola de Protecciyn de Datos (AEPD), Mario Costeja Gonzбlez (Personal data – Protection of individuals with regard to the processing of such data – Directive 95/46/EC – Articles 2, 4, 12 and 14 – Material and territorial scope – Internet search engines – Processing of data contained on websites – Searching for, indexing and storage of such data – Responsibility of the operator of the search engine – Establishment on the territory of a Member State – Extent of that operator's obligations and of the data subject's rights – Charter of Fundamental Rights of the European Union – Articles 7 and 8) // Official Journal. C 212. 7.7.2014. P. 4–5.

4. McGoldrick D. Developments in the Right to be Forgotten. *Human Rights Law Review*. 2013. V. 13/ #4. P. 761–776.

5. Opinion of Advocate General Jддskinen delivered on 25 June 2013, C-131/12 Case Google Spain SL, Google Inc. v Agencia Espacola de Protecciyn de Datos (AEPD), Mario Costeja Gonzбlez. URL: http://eur-lex.europa. Eu.

6. Frantziou E. Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos / Eleni Frantziou. *Human Rights Law Review*. 2014. No. 14. P. 761–777.

7. Кавукиан Э. Privacy by Design: 7 основополагающих принципов. URL: https://www.zakon.kz/4670977-privacy-by-design.-7.html.

8. Guidelines on Transparency under Regulation 2016/679 (wp260rev.01). [. URL: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

9. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. URL: https://eur-lex.europa.eu/eli/dir/2016/681/oj.

10. Publishers Haven't Realized Just How Big a Deal GDPR is – Baekdal Plus. URL: https://baekdal.com/strategy/publishers-havent-realized-just-how-big-a-deal-gdpr-is/

11. The Race to GDPR: A Study of Companies in the United States & Europe. URL: https://iapp.org/media/pdf/resource_center/Ponemon_race-to-gdpr.pdf

12. Structural Violation of "Right to Access" and GDPR complaints against Netflix, Amazon, Spotify, YouTube and Apple filed. URL: https://noyb.eu/wp-content/uploads/2019/01/PA_st_EN. 13. What are the compatibility issues between GDPR and blockchain? URL: https://www.siliconrepublic.com/enterprise/blockchain-gdpr-eu.

14. IBM, the GDPR and "blockchain" — whatever that word specifically means – Attack of the 50 Foot Blockchai. URL: https://davidgerard.co.uk/blockchain/2018/06/28/ibm-the-gdpr-and-blockchain-whatever-that-word-specifically-means/.

15. Here's how GDPR and the blockchain can coexist. URL: https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/.

16. Грустный закон. Как защита персональных данных влияет на блокчейн-проекты Технологии Forbes.ru. URL: https://www.forbes.ru/tehnologii/363971-grustnyy-zakon-kak-zashchita-personalnyh-dannyh-vliyaet-na-blokcheyn-proekty.

17. Julia Reda. Article 13 is almost finished – and it will change the internet as we know it . URL: https://juliareda.eu/2019/01/article-13-almost-finished/.

18. Meeting | Hearings | United States Senate Committee on the Judiciary. URL: https://www.judiciary.senate.gov/meetings/gdpr-and-ccpa-opt-ins-consumer-control-and-the-impact-on-competition-and-innovation.

19. Why the Debate Over Privacy Can't Rely on Tech Giants | Electronic Frontier Foundation. URL: https://www.eff.org/deeplinks/2019/03/why-debate-over-privacy-cant-rely-tech-giants.

Анотація

Бойко В. Д., Василенко М. Д. **Кібербезпека та захист персональних даних в ЄС: проблеми цифрового суспільства.** – Стаття.

У статті досліджено реформу ЄС щодо захисту персональних даних через призму кібербезпеки в умовах цифрового суспільства. Обговорено новації, розбіжності та протиріччя між чинним законодавством та технічним вирішенням питань захисту персональних даних.

Ключові слова: кібербезпека, захист персональних даних, обробка персональних даних, приватність, ЄС, Загальний регламент захисту даних, цифрове суспільство.

Аннотация

Бойко В. Д., Василенко Н. Д. **Кибербезопасность и защита персональных данных в ЕС: проблемы цифрового общества.** – Статья.

В статье исследована реформа ЕС по защите персональных данных через призму кибербезопасности в условиях цифрового общества. Обсуждены новации, разногласия и противоречия между действующим законодательством и техническим решением вопросов защиты персональных данных.

Ключевые слова: кибербезопасность, защита персональных данных, обработка персональных данных, конфидициальность, ЕС, Общий регламент защиты данных, цифровое общество.

S u m m a r y

Boyko V. D., Vasylenko N. D. **Cybersecurity and personal data protection in the EU: problems in digital society.** – Article.

The article explored the European Union's reform of the protection of personal data through the prism of cybersecurity and digital society. Innovations, disagreements and contradictions between current legislation and technical decision of personal data protection are discussed.

Key words: cybersecurity, personal data protection, personal data processing, privacy, EU, GDPR, General Data Protection Regulation, digital society.