УДК 347.12
DOI https://doi.org/10.32837/chc.v0i42.434

Блохін Максим Юрійович,
аспірант кафедри цивільного права
Національного університету «Одеська юридична академія»
ORCID ID: https://orcid.org/0000-0002-3922-5923

GENERAL DATA PROTECTION REGULATION (GDPR) ЯК ПОТЕНЦІЙНЕ ДЖЕРЕЛО ВДОСКОНАЛЕННЯ ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Постановка проблеми. Сучасне суспільство розвивається за графіком геометричної прогресії. Донедавна технології сприймалися та використовувалися лише як своєрідний «полегшувач» життя, адже вони допомагали людям вирішувати доволі повсякденні побутові й виробничі проблеми, мінімізуючи рівень витрат людських сил та енергії, максимально відсторонюючи людину від технічної й механічної роботи.

Але XXI століття трансформувало світ настільки, що уявити його без технологій неможливо. Технології стали невід'ємною частиною сучасного життя. На особливу увагу заслуговують ті технології, що надають індивідам доступ до різного роду інформації, яка завдяки розвитку й розповсюдженню мережі Інтернет досягла майже незліченного об'єму. Тому в рамках тотальної інформатизації повсякденного життя сучасне суспільство почало плавно (приблизно із зародженням інформаційних технологій у 60-х роках XX століття) переходити до нового етапу свого розвитку, який сучасні вчені ідентифікують як «інформаційне суспільство». У 1993 році сутність інформаційного суспільства розкрита Комісією ЄС: «Інформаційне суспільство – це суспільство, у якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку».

Варто зазначити, що далеко не вся інформація, яка знаходиться в мережі Інтернет, має бути загальнодоступною, адже користувачі інформаційних технологій, які хоча б раз під'єднуються до «всесвітньої павутини», відразу ж залишають там свій «інформаційний слід» – персональні дані, що являють собою масив унікальної індивідуальної інформації про особу-користувача. Загальнодоступність такої інформації може негативно вплинути на приватність цієї особи або навіть завдати їй великої моральної та матеріальної шкоди.

Вітчизняне законодавство, а саме Закон України «Про захист персональних даних», регулює правові відносини, пов'язані із захистом та обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини та громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Він визначає персональні дані як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Але, як показує практика, цей Закон значно поступається закордонним аналогам, таким як європейський GDPR (General Data Protection Regulation), бразильський LGPD (Lei Geral de Proteção de Dados) та інші нормативні акти у сфері регулювання захисту персональних даних, особливо в питаннях щодо відслідковування надання згоди на обробку персональних даних, забезпечення захисту персональних даних і встановлення повноважень різних суб'єктів щодо збирання й обробки персональних даних.

На додаткову увагу, на нашу думку, заслуговує саме європейський варіант урегулювання сфери захисту персональних даних, а саме GDPR.

Загальний регламент про захист даних (англ. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679) – регламент у межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Він також стосується експорту персональних даних за межі ЄС і ЄЕЗ. GDPR покликаний насамперед надати громадянам і резидентам ЄС контроль за їхніми персональними даними та спростити регуляторне середовище для міжна-

родного бізнесу шляхом уніфікації регулювання в межах ЄС [1].

Стан дослідження теми. Оскільки GDPR є доволі новим нормативним актом (прийнятий 27 квітня 2016 року та набув чинності 25 травня 2018 року), а стан дослідження сфери IT-права й інституту захисту персональних даних знаходиться на початковому етапі, у вітчизняному науковому товаристві практично відсутні роботи, у яких приділяють увагу саме темі захисту персональних даних за GDPR як одного з основних актів у цій сфері.

Метою статті є аналіз потенціалу цього нормативного акта та його окремих положень з метою ознайомлення й оцінки можливості його імплементації в сучасне українське законодавство.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Для подальшого аналізу варто більше детально розібратися, що таке GDPR, його основні положення, сфера його дії та суб'єкти, які керуються ним у діяльності.

Загальний регламенту про захист даних (General Data Protection Regulation) (далі – Регламент) установлює правила обробки персональних даних, загальні для всіх країн-учасниць, і враховує всі зміни у сфері комп'ютерних технологій, що відбулися в останні роки, які суттєво вплинули на процес обробки даних. Його завдання полягає в приведенні чинних правил обробки персональних даних у відповідність до вимог нових технологій, включаючи Інтернет, хмарні обчислення й соціальні мережі [4].

Нові правила захисту даних поширюються не тільки в межах ЄС, а й для всіх компаній, які працюють у ЄС навіть без штаб-квартири компанії в ЄС та обробляють персональні дані громадян Європи. Обробка персональних даних відбувається в момент, коли вони продають товари чи послуги людям у ЄС, або надають товари та послуги безкоштовно, або аналізують поведінку користувачів Інтернету. Окрім компаній, GDPR також поширюється на державні адміністрації, які пропонують усе більше цифрових послуг у контексті електронного уряду.

Передусім варто зазначити, що, за нормами Регламенту, споживачі завжди повністю поінформовані про те, що відбувається з їхніми даними, а також мають можливість заперечити проти обробки своїх даних. Європейський законодавець хоче проінформувати громадян про те, хто володіє їхніми даними та як вони можуть реалізувати свої права стосовно процесу збору й обробки цих даних. Для компаній (юридичний осіб) також є свої переваги: наприклад, нові зобов'язання, передбачені Регламентом, щодо видалення персональних даних можуть допомогти компаніям більш «чисто» обробляти персональні дані. Тому в разі дотримання компанією правил поводження з персональними даними це сприятиме підвищенню її ділової репутації та іміджу в цілому, а це, у свою чергу, може дати їм перевагу на конкурентному ринку.

Наступним позитивним моментом хотілося би виділити чітке розмежування «ролей» у контексті збору, обробки та використання персональних даних. Так, статтею 4 Регламенту введені такі поняття:

– *контролер даних* (англ. data controller) – фізична або юридична особа, державний орган, установа або інший орган, який самостійно або спільно з іншими визначає цілі й засоби обробки персональних даних, наприклад, соціальна мережа або служба таксі;

– *обробник даних* (англ. data processor) – це фізична або юридична особа, державний орган, установа або інший орган, який обробляє персональні дані від імені за дорученням контролера, наприклад, постачальник хмарних послуг;

– *суб'єкт даних (особа)* (англ. data subject (person)) – фізична особа, дані якої обробляються;

– *спеціальні категорії персональних даних* (англ. special categories of personal data) – дані про расу, політичну думку, релігійні або філософські переконання, генетичні дані, членство в профспілках, біометричні дані, що дають змогу визначити конкретну людину, дані про здоров'я, сексуальну орієнтацію.

Чи не найбільшим позитивним нововведенням є розширення й визначення найважливіших прав суб'єктів даних:

– *право на прозору інформацію та спілкування щодо використання персональних даних*;

– *право знати, коли збираються й обробляються персональні дані;*

– *право перевіряти збережені дані;*

– *право на виправлення даних;*

– *право на видалення даних (право на забуття).* Це право дублюється з Директиви 95/46/ЕС. Суб'єкти даних мають право на видалення будь-якої інформації про персональні дані особи (у тому числі будь-яка інформація з результатів пошуку, посилання, повідомлення тощо). Таке право суб'єктів персональних даних кореспондується обов'язком контролера здійснити

видалення подібної інформації. Будь-яка компанія, що обробляє персональні дані, зобов'язана видаляти такі дані за запитом суб'єкта таких даних, якщо це не суперечить інтересам суспільства або іншим фундаментальним правам людини [3];

– *право заборонити обробку/використання даних;*

– *право на переносимість даних.* Це право полягає в тому, що компанії зобов'язані надавати на безоплатній основі електронну копію персональних даних іншій компанії на вимогу самого суб'єкта персональних даних. Наприклад, суб'єкт даних користується сервісом «carsharing» Компанії № 1 і через деякий час суб'єкт даних виявив намір припинити користуватися послугами компанії № 1 і почав користуватися послугами «carsharing» Компанії № 2. У такому випадку право на переносимість дозволяє отримати персональні дані від Компанії № 1 і передати їх іншому сервісу, наприклад, Компанії № 2) [3];

– *право на отримання даних у портативному форматі;*

– *право на заперечення* (наприклад, пізніше);

– *право на той факт, що дані не обробляються автоматично без згоди, якщо це має юридичні наслідки* (наприклад, при оформленні страховки або заяві на кредитну картку);

– *обмеження прав*: коли існують «вищі закони», вони обмежують права суб'єкта даних. (Наприклад, строки зберігання рахунків-фактур і контрактів, національна безпека, розслідування поліції тощо.)

На особливу увагу заслуговує впровадження нормами GDPR інституту уповноваженого (офіцера) із захисту даних (англ. data protection office, або ж DPO). Усупереч поширеній думці, вирішальним для юридичного зобов'язання щодо призначення співробітника із захисту даних є не розмір компанії, а основна діяльність, пов'язана з обробкою даних, яка визначається як така, що є важливою для досягнення цілей компанії. Якщо ці основні види діяльності полягають у широкомасштабній обробці конфіденційних персональних даних або у формі обробки даних, які є особливо важливими для прав суб'єктів даних, компанія повинна призначити таку відповідальну особу. Також Регламентом передбачено, що державні органи завжди повинні призначати DPO, за винятком судів (з осіб, які працюють у судах). Крім того, законодавча норма про призначення уповноваженого із захисту даних містить положення щодо гнучкості для держав-членів Європейського Союзу. Вони мають право вирішувати, чи має компанія призначати співробітника з питань захисту даних залежно від більш жорстких вимог, передбачених національним законодавством країни-члена (наприклад, розділ 38 Федерального закону про захист даних Німеччини). Також, відповідно до Регламенту й норм національного законодавства, група підприємств може призначити одного уповноваженого із захисту даних, який охоплюватиме діяльність декількох компаній (суб'єктів) одночасно. Якщо група вирішує це зробити, то ця особа має перебувати у вільному доступі для всіх контролюючих органів, працівників і зовнішніх суб'єктів даних. Якщо жодних юридичних зобов'язань щодо захисту персональних даних не існує, компанії можуть добровільно призначити DPO для допомоги компанії або державного органу в дотриманні вимог щодо захисту даних.

Стосовно оскарження власників персональних даних щодо порушення їхніх прав, то, відповідно до Регламенту, кожна країна-член ЄС має національний (уповноважений) орган управління захистом даних (англ. data protection authority, або ж DPA). DPA несуть відповідальність за встановлення відповідності й утілення в життя відповідних законів на національному рівні, але зобов'язані бути незалежними навіть від контролю з боку власного національного уряду. Країни-члени Співтовариства можуть мати один або більше органів управління. Кожна організація може вибрати один DPA, який контролює відповідність GDPR для організації в цілому. Єдиний наглядовий орган має можливість контролювати обробку й захист даних, що забезпечуються в інших країнах-членах. Орган управління захистом даних допомагає приймати рішення в правових питаннях і може розслідувати діяльність компаній у разі порушень, припиняти роботу керуючих даними й обробників, які несуть юридичну відповідальність за порушення GDPR, і визначати штрафні санкції. Крім того, він вирішує, чи може організація передавати дані за межі ЄС, якщо так, то які механізми захисту варто застосувати. У конкретній організації основною особою, що підтримує зв'язок із DPA, буде керівник із захисту персональних даних [10].

Також постраждалі особи можуть подати скаргу до відповідального наглядового органу в ЄС (DPA) у разі виявлення ними будь-яких порушень. Якщо DPA виявлять будь-які порушення захисту персональних даних, вони в майбутньому будуть зобов'язані повідомити про це наглядові державні органи в строк протягом 72 годин.

Таким чином, повноваження наглядових державних органів значно посилюються, а тому в майбутньому, швидше за все, ми будемо бачити все більше й більше правових конфліктів між великими Інтернет-компаніями, такими як Facebook чи Google, та органами державної влади, які діятимуть в інтересах своїх громадян.

Загальноєвропейським контролюючим органом є Європейська рада з захисту даних (European Data Protection Board). Також окремо на рівні держав-членів ЄС діють регулюючі органи, які є національними регуляторами у сфері захисту персональних даних [3].

За особливо грубі порушення, перераховані в статті 83 (5) Регламенту, розмір штрафу може становити до 20 мільйонів євро або у випадку зобов'язання до 4% їх загального задекларованого обороту за попередній фінансовий рік, залежно від того яке значення буде вищим. Але навіть за менш серйозні порушення, зазначені в статті 83 (4) Регламенту, передбачено штрафи в розмірі до 10 мільйонів євро або в разі чинного зобов'язання до 2% від загального задекларованого обороту попереднього фінансового року, залежно від того яке значення буде вищим.

Висновки з дослідження та перспективи подальших розвідок у цьому напрямі. Підсумовуючи, можна з упевненістю сказати, що GDPR є найбільш розвиненим і прогресивним нормативним актом, який стосується питань захисту персональних даних. Спектр правовідносин, що регулюються цим нормативним актом, визначеність понять, екстериторіальність його дії та відсутність проблем у практичному застосуванні явно виділяються його з-поміж усіх інших світових нормативних актів, особливо порівняно з вітчизняним законодавством.

Отже, видається, що положення GDPR обов'язково мають бути використані для вдосконалення чинного законодавства, а саме виправлення його недоліків та усунення колізій, створення всіх необхідних умов для його ефективного застосування на практиці для безперешкодного захисту прав та інтересів громадян щодо захисту персональних даних. Але імплементація цього нормативного акта може потребувати багато зусиль, адже при його прийнятті законотворці опиралися на вже сформовану законодавчу базу країн ЄС і різні напрацювання у сфері інформаційної безпеки. Звісно, такі зміни будуть уноситися саме до вже чинного Закону України «Про захист персональних даних», який не є настільки розвиненим, і все ж таки при раціональному опрацюванні вищезазначених позитивних сторін українське законодавство у сфері кібербезпеки може зазнати значних і вагомих поліпшень.

ЛІТЕРАТУРА:

1. Drexl J. Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy. *Max Planck Institute for Innovation & Competition Research Paper.* 2018. № 18–23.
2. Presidency of the Council: «Compromise text. Several partial general approaches have been instrumental in converging views in Council on the proposal for a General Data Protection Regulation in its entirety. The text on the Regulation which the Presidency submits for approval as a General Approach appears in annex», 201 pages, 11 June 2015.
3. Гвоздій В.А. General Data Protection Regulation. URL: http://unba.org.ua/publications/3320-general-data-protection-regulation.html.
4. Грибанов А. А. Общий регламент о защите персональных данных (General Data Protection Regulation): идеи для совершенствования российского законодательства. *Закон.* 2018. № 3. С. 149–162. URL: https://urfac.ru/?p=437.
5. Згода суб'єкта персональних даних. *Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції* / А.Г. Чубенко, М.В. Лошицький, Д.М. Павлов, С.С. Бичкова, О.С. Юнін. Київ : Ваіте, 2018. С. 280.
6. Крылова М.С. Принципы обработки персональных данных в праве Европейского Союза. *Актуальные проблемы российского права.* 2017. № 10. С. 175–181.
7. Про захист персональних даних : Закон України № 2297-VI (2010). URL: https://zakon.rada.gov.ua/laws/show/2297-17.
8. Про інформацію : Закон України № 2657-XII (1992). URL: https://zakon.rada.gov.ua/laws/show/2657-12.
9. Регламент (ЄС) 2016/679 Європейського парламенту та Ради 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. URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es 2016679.pdf.
10. Роджер А. Граймз. Как защитить персональные данные в соответствии с GDPR. *CSO.* 2017. 14 августа. URL: https://www.osp.ru/cio/2017/07/13052957.
11. Сопілко І.М. Становлення інформаційного суспільства та інформаційні загрози в мережі Інтернет. *Юридичний вісник.* 2017. № 3 (44).
12. Гуз А.М., Касперський І.П., Ткачук Т.Ю. Організація захисту інформації з обмеженим доступом : навчальний посібник. Київ : НА СБУ, 2018. С. 33–58.
13. Ткачук Т.Ю., Довгань О.Д. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право.* 2018. № 2 (25). С. 73–85.

Блохін Максим Юрійович

GENERAL DATA PROTECTION REGULATION (GDPR) ЯК ПОТЕНЦІЙНЕ ДЖЕРЕЛО ВДОСКОНАЛЕННЯ ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття присвячена питанням захисту персональних даних у мережі Інтернет нормативним актом Європейського Союзу – GDPR (General Data Protection Regulation) – і його позитивним сторонам, які можна імплементувати у вітчизняне законодавство з метою його вдосконалення. Так як цей регуляторний акт уже широко використовується в Європі певний період часу, то відслідкувати рівень його дієвості можна на реальній практиці застосування GDPR країнами-членами Європейського Союзу. Розглянуто передумови виникнення цього закону та його прийняття Європейським Союзом, визначено термін «інформаційне суспільства» та його значимість у виникненні цих передумов. Повністю розглянуто сферу дії цього акта та його особливості врегулювання питань захисту персональних даних. Проаналізовані дефініції нових понять та інститутів, запропонованих цим нормативним актом, такі як контролер даних, обробник даних, суб'єкт даних (особа), спеціальні категорії персональних даних. Окреслено рамки дії цього нормативного акта (суб'єктні, темпоральні, територіальні тощо). Проведено дослідження особливості структури цього акта (у вигляді, актуальному на момент написання статті). Охарактеризовано ексклюзивні види прав, які введені цим нормативним актом, такі як право на видалення даних (право на забуття), право на переносимість даних, та інші види прав, передбачені GDPR. Визначено ліміти відповідальності суб'єктів і штрафні санкції, які застосовуються в разі вчинення суб'єктами порушень різних рівнів у сфері захисту персональних даних. Описано роль уповноваженого (офіцера) із захисту даних (або ж DPO). Проаналізовано окремі його положення, які заслуговують на особливу увагу. Визначено характерні риси цього акта, які відрізняють його від інших світових аналогів. Описано процедуру звернення постраждалих осіб з метою захисту своїх порушених прав та інтересів у сфері захисту персональних даних. Охарактеризовано його значимість для розвитку світового регулювання інституту захисту персональних даних і всіх суміжних правовідносин.

Ключові слова: IT-право, GDPR, захист персональних даних, використання персональних даних, інформаційна безпека, кібербезпека, інформаційне законодавство.

Blokhin Maksym

GENERAL DATA PROTECTION REGULATION (GDPR) AS POTENTIAL SOURCE OF IMPROVEMENT OF THE DOMESTIC LEGISLATION IN THE SPHERE OF PERSONAL DATA PROTECTION

The article is devoted to the protection of personal data in the Internet by the normative act of the European Union – GDPR (General Data Protection Regulation) and its positive aspects, which can be implemented in domestic legislation in order to improve it. Since this regulatory act has been widely used in Europe for some time, it is possible to trace the level of its effectiveness in the actual practice of application of the GDPR by the member states of the European Union. The preconditions for the emergence of this law and its adoption by the European Union are considered, the term "information society" and its significance in the emergence of these preconditions are defined. The scope of this act and its features of regulation of personal data protection are fully considered. The definitions of new concepts and institutions proposed by this normative act, such as data controller, data processor, data subject (person), special categories of personal data are analyzed. The scope of this normative act (subjective, temporal, territorial and others) is outlined. A study of the peculiarities of the structure of this act (in the form relevant at the time of writing). The exclusive types of rights introduced by this normative act, such as the right to delete data (right to be forgotten), the right to data portability and other types of rights provided by the GDPR are described. The limits of responsibility of subjects and penalties which are applied in case of commission by subjects of infringements of various levels in the field of protection of personal data are defined. The role of the Data Protection Officer (or DPO) is described. Some of its provisions that deserve special attention are analyzed. The characteristic features of this act that distinguish it from other world analogues are determined. The procedure for appealing to victims in order to protect their violated rights and interests in the field of personal data protection is described. The significance for the development of global regulation of the institute of personal data protection and all related legal relations is described.

Key words: IT law, GDPR, personal data protection, use of personal data, information security, cybersecurity, information legislation.