8. Case of Yankov v. Bulgaria, Application №39084/97. Council of Europe: European Court of Human Rights, 11 December 2003. URL:http://hudoc.echr.coe.int/eng?i=001-61539.

Надійшла до редакції 23.11.2018

SUMMARY

Kuchuk A.M. Soviet Legality v. Human Dignity (on Materials of Individual Decisions of the European Court of Human Rights). The article focuses on the need setting off the Soviet concept of legality and recognition the system of human dignity as the basis. One of the significant tasks of domestic jurisprudence is the advancing abandonment of the prevalence of normative understanding of law and the implementation of the concepts of the natural law school (a significant part of which is enshrined in the Constitution of Ukraine). Normative understanding of law in its Soviet treatment as the basis of legal superstructure recognized the will of the ruling class, which was fixed in precriptive texts and which was enforced by the state apparatus with its inherent in hierarchical subordination. At the same time, the purpose of building up socialism was to use by such a state apparatus of any means. The main thing was to comply with the letter of the law (and by-law), even if it restricted / violated human rights (which were not recognized as such and were denied). Therefore, the main attention of scholars and practitioners was focused precisely on the letter of law, formal prescriptions, dogmas of the Soviet jurisprudence, which, moreover, did not provide for a proper argument for a solution to a legal conflict.

It is noted that legal practice is still largely derived from the Soviet legal dogmas (as well as a significant part of the scholars).

The individual judgments of the European Court of Human Rights, which reasoning is based on human dignity, are analyzed. A detailed analysis of the judgment of the European Court of Human Rights in Vinter and others v. the United Kingdom is provided. The court explained for the first time that the prisoner for life has the right to know, at the beginning of his sentence, what he must do to qualify for release, and under what conditions, including when there is a review of his sentence, or when such a review can be to petitio.

It is emphasized that recognition of human dignity involves the recognition of equal opportunities of individuals and the need for a tolerant attitude to each other.

It is concluded that in today's conditions of development of a civilized society, the basis of jurisprudence should be human dignity, which requires a radical reassessment of the axiological foundations of relations in society and changes in the domestic legal paradigm.

Keywords: *European Court of Human Rights, human dignity, human rights, the rule of law, Soviet legality.*

УДК 342.72/.73

Серьогін В.О.
доктор юридичних наук, професор
(Харківський національний університет ім. В.Н. Каразіна)

DOI: 10.31733/2078-3566-2018-5-91-99

РЕФОРМА СИСТЕМИ ЗАХИСТУ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ: ПРИЧИНИ ТА НОВАЦІЇ

Висвітлено ключові зміни, до яких призведе новий Загальний регламент про захист даних, що набув чинності з травня 2018 року. Здійснено спробу критичного аналізу цієї реформи та оцінки деяких її наслідків, а також спробу розглянути їх у більш широкому контексті цифрової економіки та управління нею.

Ключові слова: *недоторканність приватного життя, інформаційне прайвесі, персональні дані, захист персональних даних.*

Постановка проблеми. Через майже п’ять років інтенсивної роботи, що супроводжувалася палкими політичними дискусіями та широким соціальним розголосом, реформа захисту даних ЄС, нарешті, стала реальністю. Нова структура складається із Загального регламенту про захист даних (англ. General Data Protection Regulation, GDPR; Regulation (EU)

© Серьогін В.О., 2018

2016/679) [1], який замінив Директиву 95/46/ЕС про захист даних [2], та нової Директиви про захист фізичних осіб стосовно обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або кримінального переслідування у справах про кримінальні правопорушення чи виконання кримінальних покарань [3]. Обидва документи набули чинності з травня 2018 р. [4]. Реформа має на меті модернізацію та гармонізацію захисту даних на всій території ЄС та є важливим елементом більш широкої та особливо амбітної Стратегії єдиного цифрового ринку [5], яку ЄС розпочав паралельно і чиї далекосяжні наслідки розкриватимуться протягом найближчих років.

Аналіз публікацій, в яких започатковано розв'язання даної проблеми. Реформа захисту даних, проведена в ЄС, отримала жваву реакцію серед зарубіжних фахівців у сфері обробки інформації та захисту інформаційного прайвесі. Серед останніх праць, опублікованих за даною тематикою, варто зазначити дослідження Р. Вебера, Б. Енгельс, Д. Ердоса, Х. Кунера, В. Мейєр-Шонбергера, Н. Пуртової, М. Рустада, Д. Хофмана та ін. Втім, суттєва новизна застосованих у Загальному регламенті підходів та відсутність усталеної практики його застосування роблять дану проблематику відкритою для аналізу.

Метою даної статті є висвітлення ключових змін, до яких призведе Загальний регламент про захист даних. Ми спробуємо критично проаналізувати цю реформу та оцінити деякі її наслідки, а також розглянути їх у більш широкому контексті цифрової економіки та управління нею.

Виклад основного матеріалу. Причини для реформи є багатоманітними. Одні з них мають загальний характер і стосуються внутрішнього бажання запроваджувати технічні новації для забезпечення кращого та більш ефективного досягнення ключових суспільних цілей у новій обстановці (див.: [6]). Директива ЄС про захист даних діяла з 1995 р. Вона майже заслуговує на означення «стародавньої» у такому специфічному середовищі, як цифрове, особливо враховуючи радикальні перетворення, котрі відбулися після комерціалізації Інтернету в середині 1990-х років.

У теперішній час стало очевидним, що, поруч із суттєвими позитивними перетвореннями, цифрові технології також призвели до невідомих раніше ризиків прайвесі, які виникли внаслідок оперативного збору, обробки, зберігання та використання даних. Окремою причиною занепокоєння в колах ЄС стало те, наскільки легко стало переміщувати дані через кордони держав. Як наслідок, також було чітко усвідомлено складність застосування законів про захист прайвесі в іноземних юрисдикціях.

Занепокоєння полягало у тому, що ця комбінація в кінцевому підсумку серйозно підриває прайвесі громадян ЄС [7]. Важливо підкреслити насамперед, що право на повагу до приватного життя є ключовою концепцією в законодавстві ЄС, оскільки відображає глибокі культурні цінності та концепції. Ґрунтуючись на Європейській конвенції про захист прав людини і основоположних свобод 1950 р., яка захищає право на приватне та сімейне життя у ст. 8, Хартія основних прав Європейського Союзу (далі − Хартія) [8] розрізняє право на повагу до приватного та сімейного життя (ст. 7) та право на захист персональних даних (ст. 8). Ця відмінність не є випадковою, адже відображає підвищену стурбованість ЄС та перетворюється на позитивний обов'язок держав [9] здійснювати ефективний захист персональних даних і регулювати їх передачу. Директива про захист даних була важливою частиною тогочасної політики ЄС. Оскільки середовище, котре піддавалося регулюванню, вже суттєво змінилося, зокрема, в частині використання та ролі даних в економіці та інших сферах суспільного життя (див.: [10]), Директива терміново вимагала оновлення, щоб забезпечити достатній рівень захисту прайвесі. Необхідність більш активного залучення ЄС як наднаціонального утворення також була зумовлена тими змінами, що випливали з Лісабонського договору, який набрав чинності в 2009 р. [11].

Важливим, хоч і не безпосереднім, поштовхом у даній сфері, безумовно, було викриття, зроблене в 2013 р. Е. Сноуденом, яке виявило широту і глибину стеження з боку Агентства національної безпеки США (NSA), що, до речі, також передбачало доступ до даних мільйонів приватних користувачів, у тому числі у системах Google, Facebook, Apple та інших великих інтернет-гравців, що базуються в США. Більш конкретними факторами впливу стала серія рішень Суду ЄС, що призвела до важливих змін в існуючій юридичній практиці та загальному розумінні європейцями права особи на захист в Інтернеті.

Коротко оглянемо ці рішення у хронологічному порядку їх прийняття.

Першою такою справою стала добре відома, хоч і, мабуть, дещо оманлива справа під назвою «право бути забутим». Вона стосується рішення, прийнятого Судом ЄС у

2014 р. проти Google Spain та Google Inc. [12]. Фактичним позивачем у цій справі був М. Костеха Гонсалес, тепер широко відомий. Він домагався вироку суду, який би забороняв пошуковій системі Google показувати посилання на газетну статтю, опубліковану в 1998 р., коли його ім'я згадувалося в негативному контексті. У статті йшлося про проведення аукціону й арешт будинку пана Гонсалеса для стягнення його боргів. Пан Гонсалес стверджував, що ці процедури були повністю реалізовані ще кілька років тому, і посилання на них тепер не має значення.

Суд ЄС визнав Google «контролером» персональних даних, оскільки кваліфікував збір і зберігання інформації в Інтернеті як обробку пошуковими системами цієї інформації, як це визначено Директивою 95/46/ЕС. Суд постановив, що особа має право заперечувати зв´язок пошукової системи з персональними даними, і оцінка такого заперечення вимагає збалансування прав та інтересів, у контексті яких слід враховувати значення прав суб'єкта даних, що випливають зі статей 7 та 8 Хартії. Оператори пошукових систем зобов'язані видаляти посилання на веб-сторінки з їхнього списку результатів, якщо це вимагається суб'єктом даних, на тій підставі, що така інформація більше не повинна бути пов'язана з його іменем за допомогою такого списку. У цьому контексті, навіть спочатку законна обробка точних даних може з часом стати несумісною з Директивою, якщо дані більше не є необхідними у світлі цілей, для яких вона була зібрана чи оброблена.

Справа Google Spain справила серйозні наслідки для пошукових систем і для ролі інтернет-провайдерів у більш загальному розумінні. Вона надала змогу окремим особам захищати свої права у відносинах з провайдерами, а також глибоко вплинула на глобальну доступність та потоки інформації в Інтернеті. У подальшому «право бути забутим» стало одним із центральних елементів палітри прав користувачів Інтернету, передбачених у Загальному регламенті.

Значно менш відомим є ще одне рішення Суду ЄС 2014 р., яким було визнано нечинною Директиву 2006/24/ЄС про зберігання даних [13]. Прийняття згаданої Директиви [14] було політично зумовлене терористичними атаками в Мадриді (2004 р.) та Лондоні (2005 р.), спрямовувалося на забезпечення гармонізації законодавства держав-членів та вимагало зберігання даних зі стаціонарної, мобільної або Інтернет-телефонії, а також повідомлень електронної пошти протягом щонайменше шести місяців, а за певних обставин − до двох років. Така вимога була спрямована на те, щоб забезпечити доступність відповідних даних для цілей розслідування, виявлення та переслідування осіб, винних у вчиненні тяжких злочинів, визначених кожною державою-членом у своєму національному законодавстві. Зберігання не вимагало конкретної підозри щодо теми, і воно здійснювалося в багатьох аспектах, іноді дуже суперечливих. Усі ці суперечності були припинені рішенням Суду ЄС в Digital Rights Ireland.

Суд визнав, що Директива тягне за собою широке і серйозне втручання у статті 6 та 7 Хартії. Хоча Суд ЄС і констатував, що втручання відповідає меті загального інтересу, сприяючи боротьбі із серйозними злочинами, а отже, і громадській безпеці, однак визнав, що таке втручання не є пропорційним досягненню цілей Директиви, оскільки не розрізняє різні засоби комунікації, різні види даних або різні типи користувачів. Крім того, не було визначено сутність та процедурні умови доступу до даних; також не було окреслено об'єктивних критеріїв визначення встановленого періоду зберігання. Також Директива не передбачала жодних адекватних гарантій для забезпечення ефективного захисту даних, що зберігаються, від ризику зловживання та проти будь-якого незаконного доступу до цих даних та використання цих даних.

Хоча ця справа була менш обговорюваною, зокрема в популярних засобах масової інформації, вона виявила ще одну прогалину в загальній структурі захисту даних ЄС. Суд також чітко позначив небезпеку, пов'язану зі збором великих даних (англ. Big Data), наприклад, вказав, що вона дозволяє робити дуже точні висновки щодо приватного життя окремих осіб, і визнав той факт, що збереження даних у такий спосіб може мати «приголомшливий» вплив на право на свободу вираження поглядів. У кінцевому рахунку це ще раз підтвердило неабияку складність досягнення правильного балансу між основним правом на захист персональних даних та наданням даних для інших важливих та обґрунтованих цілей, таких як захист національної безпеки та його особливо гостру і актуальну підтему боротьби з тероризмом.

Третя справа, яка багато в чому змінила правову ситуацію та вимагала змін у законодавстві ЄС, − це справа Шремса (Schrems), рішення за якою було винесено 6 жовтня

2015 р. [15]. М. Шремс, громадянин Австрії, подав позов проти ірландського контролюючого органу (Комісара з питань захисту даних) після того, як той відхилив його скаргу на практику Facebook зберігати дані користувача у США. Позивач стверджував, що його дані не були належним чином захищені від викриття з боку американського АНБ, незважаючи на існуючу між ЄС та США угоду − так звану схему «безпечної гавані» (англ. «safe harbor»), яка безпосередньо вимагала надавати Сполученим Штатам персональні дані тільки за умови забезпечення належного рівня їх захисту [16]. Визначати цю відповідність рівня захисту внутрішньому законодавству країни чи міжнародним зобов'язанням мала Європейська комісія.

Схема «безпечної гавані» містила низку принципів щодо захисту персональних даних, на які американські підприємства могли погоджуватися на добровільній основі. Ця угода була результатом серйозних політичних дискусій і являла собою політичний компроміс, за допомогою якого намагалися подолати суттєво відмінні поняття прайвесі та його регулювання в ЄС та США.

У справі Шремса Суд ЄС зробив принаймні два висновки, які були визначальними для подальшої практики захисту даних в ЄС та її трансатлантичного виміру. Суд визнав, що існування рішення Комісії, яке визнає, що третя країна забезпечує належний рівень захисту, не може усунути чи зменшити повноваження національних наглядових органів щодо нагляду та оцінки адекватності захисту даних відповідно до Хартії та Директиви щодо захисту даних.

Крім того, Суд зауважив, що схема «безпечної гавані» застосовується виключно до американських підприємств, які дотримуються її, але не пов'язує державні органи США. Також було очевидним, що національна безпека США, суспільні інтереси та вимоги до правоохоронних органів переважають над угодою про «безпечну гавань», тож насправді американські підприємства не можуть без обмежень брати до уваги правила, встановлені цією схемою, якщо вони суперечать таким інтересам і вимогам, що також впливає на основні права громадян ЄС. Рішення Комісії не посилалося на існування будь-яких американських правил, призначених для обмеження такого втручання; також не розглядалася наявність ефективного правового захисту від втручання.

Що стосується рівня захисту, суттєво еквівалентного основним правам і свободам, гарантованим у ЄС, то суд визнав, що законодавство не обмежується тим, що є суто необхідним, тобто не відповідає вимогам пропорційності до законодавства ЄС. Суд дійшов до цього висновку, оскільки законодавство США дозволяє на загальних підставах зберігати всі персональні дані всіх осіб, дані яких передаються з ЄС до Сполучених Штатів, без будь-якої диференціації, обмеження чи виключення з урахуванням існуючої мети і без встановлення об'єктивних критеріїв для визначення меж доступу державних органів до даних та подальшого їх використання. Крім того, суд зауважив, що законодавство, яке не передбачає можливостей будь-якої особи для здійснення правового захисту від доступу до своїх персональних даних або для отримання виправлень чи стирання таких даних, ускладнює реалізацію основного права на ефективний судовий захист. З усіх цих причин Суд визнав недійсним рішення щодо «безпечної гавані».

Наведені вище три основні рішення Суду ЄС яскраво продемонстрували недоліки тогочасної системи захисту даних в ЄС та її впровадження в юрисдикціях держав-членів. Крім того, ці рішення виявили багато аспектів проблеми управління, з якими ми закономірно стикаємося, коли прагнемо до захисту прайвесі в цифрову епоху, та пов'язані з ними труднощі в узгодженні достатньо ефективного захисту даних з іншими критичними інтересами, як-от забезпечення вільного руху інформації як основи нової цифрової економіки чи створення передумов для свободи вираження поглядів в Інтернеті.

Тепер розглянемо основні зміни, що відбудуться у зв'язку із запровадженням Загального регламенту про захист даних ЄС. Деякі з них є реакцією на вищезгадані рішення Суду ЄС і здебільшого спрямовані на створення відповідного «нормативного дизайну» щодо захисту даних в Європі.

Із самого початку важливо зазначити, що Загальний регламент відображає складність не тільки самого предмета регулювання, але й сучасної економіки. Він містить у собі численні ініціативи з боку лобістських структур від промисловців та інститутів громадянського суспільства, а також положення, що стали результатом гострих дискусій між Європейською комісією, Європейською радою та Європейським парламентом. Ці дискусії ще більш загострювалися через різне сприйняття та розуміння того, що таке

прайвесі та як воно має бути захищене в різних державах-членах ЄС. Усе це пояснює тривалість процедури складання та прийняття Загального регламенту, а також компромісність його остаточного тексту.

Говорячи про позитивні риси Загального регламенту, передусім слід відзначити *більш високий рівень гармонізації*. Для цього обрано нову форму закріплення відповідних норм: на відміну від попередніх правил, котрі закріплювалися в Директиві, нові оформлені у вигляді Загального регламенту. Хоча обидва типи правових актів ЄС можуть у принципі забезпечувати високий рівень гармонізації в усіх державах-членах, регламент застосовується безпосередньо і не вимагає додаткового внутрішнього впровадження (тоді як директива визначає досягнуті результати, залишаючи вибір засобів для їх досягнення державам-членам). Крім того, норми регламенту негайно стають частиною національної правової системи, мають юридичну чинність, незалежну від національного законодавства, і навіть переважають за юридичною силою національні закони в разі колізії. Загалом, це гарантує більш високий рівень гармонізації та зменшує кількість відмінностей між державами-членами, дисциплінує деякі держави-члени (такі, як Ірландія), за їх відносно м'яке виконання правил захисту даних (особливо стосовно Facebook). Така посилена гармонізація і тим самим гарантований еквівалентний рівень захисту також відповідає згаданій вище стратегії ЄС щодо Цифрового єдиного ринку, яка спрямована на створення спрощеної, безперервної та ефективної структури для цифрової економіки в усьому ЄС та надання їй конкурентних переваг у глобальному просторі.

Незважаючи на різну форму, Загальний регламент слугує тій самій меті, що й Директива із захисту даних, і спрямований на гармонізацію захисту основних прав і свобод фізичних осіб щодо обробки персональних даних та забезпечення вільного переміщення таких даних між державами-членами. Загальний регламент містить чіткий набір принципів для досягнення цих цілей. Так, у ст. 5 зазначено, що персональні дані повинні оброблятися законно, справедливо та прозоро щодо суб'єкта даних (*принцип законності, справедливості та прозорості*); мають бути зібрані для конкретних, чітких та законних цілей (*принцип обмеження мети*); обробка повинна бути адекватною, релевантною та обмежуватись необхідними даними (*принцип мінімізації даних*); оброблювана інформація має бути точною та, де це необхідно, актуальною (*принцип точності*); дані повинні зберігатися у формі, яка дозволяє ідентифікувати суб'єктів даних не більше, ніж це необхідно для цілей, для яких обробляються персональні дані (*принцип обмеження зберігання*); обробка даних має бути надійною (*принцип цілісності та конфіденційності*); контролер даних повинен бути відповідальним (*принцип підзвітності*).

З більш як вісімдесяти сторінок тексту Загального регламенту ми зосередимо свою увагу на трьох окремих сферах, де є помітні зміни і які мають суттєво вплинути на цифрове мережеве середовище. До них належать: 1) більший захист, наданий користувачам та їхнім даним; 2) підвищена відповідальність суб'єктів контролю та обробки даних; 3) більш чітке розуміння території дії.

Якщо говорити про посилення прав споживачів, то, можливо, найбільш гостро обговорювана зміна − це запровадження у ст. 17 Загального регламенту «права бути забутим». Останнє являє собою певне розширення «права на стирання», передбаченого ст. 12 (b) Директиви про захист даних. Зокрема, суб'єкт даних може тепер стирати свої персональні дані та більше не обробляти їх, коли вони більше не є необхідними для цілей, для яких вони були зібрані; коли суб'єкт даних відкликає свою згоду або заперечує проти обробки персональних даних стосовно нього, або коли обробка його персональних даних інакше суперечить Загальному регламенту. Статті 17 (3) та 65 викладають це право у певному контексті та уточнюють, що воно не є абсолютним. Подальше зберігання персональних даних може бути законним, якщо це необхідно для здійснення права на свободу вираження поглядів та інформації, для виконання юридичного зобов'язання або для інших способів використання в інтересах суспільства, наприклад, у сфері охорони здоров'я чи наукових досліджень.

«Право бути забутим» дещо посилюється, однак, порівняно з рішенням Google Spain, оскільки воно передбачає зобов'язання контролера, який зробив персональні дані публічними, інформувати інших контролерів, що обробляють такі персональні дані, для видалення будь-яких посилань на ці дані, копій або реплік цих особистих даних. При цьому контролер має вживати обґрунтовані кроки, у тому числі наявні технології та засоби, доступні для контролера, включаючи технічні заходи.

«Право бути забутим», як зазначено в Загальному регламенті, є лише частиною значно ширшого пакета прав споживачів, що містяться в главі III Хартії і, в кінцевому рахунку, призначені для надання користувачам більшого контролю над своїми даними. Особливо привабливими доповненнями до набору прав користувача є право на прозорість інформації, право доступу до персональних даних, право на портативність даних і право на об'єкт. Існує також нове спеціальне право − не бути предметом рішення на основі автоматизованої обробки, включаючи профілювання, що здійснює правовий чи інший суттєвий вплив на користувача. Включення цієї нової гарантії було зумовлено поточними дискусіями щодо ролі алгоритмів та інших інформаційних посередників у всіх аспектах суспільного життя, а також здатністю користувачів зрозуміти та контролювати їх. Це право може бути обмежене, коли рішення: а) необхідні для договірних відносин між суб'єктом даних та контролером даних; б) дозволено законодавством ЄС або державами-членами, яким підпорядкований контролер; в) на основі явної згоди суб'єкта даних (ст. 57–66 Загального регламенту).

Таким, що не існувало під назвою «Захист даних», є положення про портативність («переносимість») даних. Після гарячих дебатів між установами ЄС та зацікавленими сторонами про те, чи відповідає таке правило регулюванню захисту даних взагалі та яким має бути його форма, те, що зараз міститься в Загальному регламенті, є достатньо потужним правом користувачів отримувати свої персональні дані у структурованому, широко вживаному і машиночитаному форматі. Користувачі можуть передавати ці дані іншому контролеру без перешкод від контролера, якому надані персональні дані (ст. 20 (1)). Якщо це технічно можливо, суб'єкт даних має право мати дані, передані безпосередньо від одного контролера до іншого (ст. 20 (2)). Хоча «переносимість» даних може здатися чудовим інструментом, який надає владу користувачам і підриває домінування ринку та пов'язані з цим сильні мережеві ефекти деяких гравців на цифровому ринку (таких як пошукові системи або сайти соціальних мереж), він повинен використовуватися з обережністю. «Переносимість» даних також може перешкоджати інноваціям, роблячи дані доступними і завдаючи шкоди саморегулюючим силам ринку.

Умови згоди, як важливий елемент для обробки даних, також були змінені, можливо, на користь користувача. Так, наприклад, відповідно до ст. 7 Загального регламенту, запит на згоду має бути представлений таким чином, що чітко відрізняється від інших запитань, є зрозумілим та легко доступним за формою й використовує чітку та зрозумілу мову. Крім того, суб'єкт даних має право відкликати свою згоду в будь-який час.

Водночас Загальний регламент призведе до суттєвих змін в обов'язках посередників − не тільки в тому, за що вони відповідають, але й у самій відповідальності. Згідно з Директивою про захист даних, існувала відмінність між контролерами даних та операторами обробки даних.

Контролером даних називалася особа чи організація, яка визначає цілі або засоби обробки персональних даних; натомість оператор даних був визначений як особа чи організація, яка просто виконує обробку даних від імені контролера даних. Ця відмінність була надзвичайно важливою, оскільки лише контролер даних виконував зобов'язання щодо захисту даних і ніс відповідальність за порушення. Протягом багатьох років це розмежування піддавалося серйозній критиці, особливо з огляду на дедалі більш складні відносини щодо обробки даних; не завжди було зрозуміло, хто визначає, для чого і як обробляються дані, а деякі суб'єкти могли позбутися відповідальності за свої дії, використовуючи правові лазівки [17, с. 6].

Загальний регламент підтримує відмінність між контролерами даних та операторами обробки даних (ст. 4 (7) і (8)), але вводить зобов'язання для обох (ст. 30 (2), 31, 32 (1) та ін.). Така відмінність також застосовується прагматично, і визнається можливість створення множинних, спільних та спів-контролерів. На контролерів даних загалом накладається більший тягар відповідальності: він несе відповідальність за забезпечення того, щоб обробка даних відповідала положенням Загального регламенту і має бути здатен продемонструвати це дотримання.

Стаття 25 Загального регламенту передбачає нове зобов'язання під назвою «захист даних за проектом та за замовчуванням» («data protection by design and by default»): контролер зобов'язаний, беручи до уваги сучасний стан, вартість реалізації, а також характер, масштаб, контекст і цілі обробки, а також пов'язані з цим ризики для прав і свобод фізичних осіб, здійснювати належні технічні та організаційні заходи (як-от псевдо-

німізація), призначені для реалізації принципів захисту даних (наприклад, для мінімізації даних), та інтегрувати необхідні гарантії до процесу обробки, щоб відповідати вимогам цього Регламенту та захищати права суб'єктів даних (ст. 25 (1)). Контролер також повинен здійснити відповідні технічні та організаційні заходи для забезпечення того, щоб за замовчуванням оброблялися лише персональні дані, необхідні для кожної конкретної мети обробки. Цей обов'язок стосується як обсягу зібраних персональних даних, так і обсягу їх обробки, періоду їх зберігання та доступності. Зокрема, такі заходи повинні забезпечити, щоб за замовчуванням персональні дані не були доступними для необмеженої кількості фізичних осіб без втручання особи (ст. 25 (2)).

Якщо тип обробки, зокрема використання нових технологій, може призвести до високого ризику для прав та свобод фізичних осіб, контролер тепер зобов'язаний провести оцінку впливу передбачених операцій обробки на захист персональних даних (ст. 35). Ця так звана «оцінка впливу на захист даних» («data protection impact assessment» − DPIA) повинна містити систематичний опис передбаченої обробки, оцінку необхідності та пропорційності обробки у зв'язку з її цілями та оцінку ризиків для прав та свобод суб'єктів даних, а також способи їх вирішення, включаючи гарантії.

Варто зазначити, що DPIA добре вибудована в інституційному плані. Отже, наглядовий орган, який повинен бути створений у кожній державі-члені, відповідає за складений перелік видів обробки операцій, що підпадають під дію DPIA. Контролер повинен проконсультуватися з наглядовим органом перед обробкою, де DPIA вказує на те, що обробка призведе до високого ризику. Протягом восьми тижнів з моменту отримання запиту про консультацію, наглядовий орган повинен надати письмові рекомендації контролеру та, де це можливо, оператору. Наглядовий орган може встановлювати різні заходи, включаючи, наприклад, тимчасове чи остаточне обмеження, чи навіть заборону на обробку (ст. 58).

Загальним регламентом передбачено низку інших механізмів, таких як необхідність деяких контролерів (наприклад, тих, що обробляють конфіденційні дані або у великих масштабах) призначати посадових осіб із захисту даних та приймати власні кодекси поведінки та схеми сертифікації, які передбачають більше можливостей дисциплінувати, хоча і м'яко, контролерів даних. Загалом вони також забезпечуватимуть кращий баланс інтересів та постійний і більш ретельний контроль даних у Європі. Водночас наглядові органи мають «жорсткі» інструменти для втручання, що охоплюють слідчі, коригувальні, дозвільні та консультативні повноваження. Залежно від порушення, органи захисту даних тепер можуть також застосовувати набагато більші штрафи − вони можуть становити до 20 млн. євро або, у випадку підприємства, до 4 % від загального обсягу річного обороту за попередній фінансовий рік, залежно від того, що вище (ст. 83 (5) і (6)).

Проведене дослідження дає змогу зробити такі **висновки**:

1. Законодавство про захист даних у ЄС пройшло через важливу реформу. В її основі лежать три найважливіші рішення Суду ЄС: у справах Google Spain, Digital Rights Ireland та Schrems.

2. Загальний регламент про захист даних (2016 р.) містить чіткий набір принципів обробки даних; до них належать принципи: а) законності, справедливості та прозорості; б) обмеження мети; в) мінімізації даних; г) точності; д) обмеження зберігання; е) цілісності та конфіденційності; є) підзвітності.

3. До найбільш суттєвих змін, передбачених Загальним регламентом, які мають суттєво вплинути на цифрове мережеве середовище в Європі, можна віднести: 1) більший захист, наданий користувачам та їхнім персональним даним; 2) підвищена відповідальність суб'єктів контролю та обробки даних; 3) більш чітке розуміння територіальних меж його дії.

4. Найбільш гостро обговорюваною зміною в законодавстві про захист даних є запровадження у ст. 17 Загального регламенту «права бути забутим». Істотною новелою є також положення про портативність (переносимість) даних, що передбачає право користувачів отримувати свої персональні дані в структурованому, широко вживаному і машиночитаному форматі.

Чи зміниться регуляторне середовище в наступні пару років після набуття чинності Загальним регламентом, чи призведе він до посилення захисту даних − усе це становить предмет подальших досліджень у даній сфері. Адже політикам доведеться ще впродовж багатьох років замислюватися про наслідки здійснених реформ і виробляти кращі та більш сміливі рішення, здатні узгодити окремі основні права людини зі зроста-

ючим попитом на транскордонні потоки даних. Стратегія ЄС щодо Цифрового єдиного ринку має значні амбіції у цьому напрямку, але деякі з основних її ініціатив ще потребують конкретних рішень.

Бібліографічні посилання

1. Regulation 2016/679 of the European Parliament and of the Council of April 27, 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), OJ L [2016] 119/1.
2. Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L [1995] 281/31.
3. Directive 2016/680 of the European Parliament and of the Council of April 27, 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, OJ L [2016] 119/89.
4. The GDPR entered into force on May 24, 2016 and will be effective as of May 25, 2018; Directive 2016/680 entered into force on May 5, 2016, and will be effective as of May 6, 2018.
5. A Digital Single Market Strategy for Europe: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (SWD(2015) 100 final). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192& from=EN.
6. Regulating technologies: legal futures, regulatory frames and technological fixes / Brownsword R., Yeung K., eds. Oxford: Hart, 2008. 408 p.
7. Future of Privacy Forum. The US-EU Safe Harbor: An Analysis of the Framework's Effectiveness in Protecting Personal Privacy. December 2013. Accessed September 8, 2016. URL: http://www.futureofprivacy.org/wp-content/ uploads/FPF-Safe-Harbor- Report.pdf..
8. Charter of Fundamental Rights of the European Union. *OJ C* [2010] 83/2.
9. European Court of Human Rights, *Refah Partisi (The Welfare Party) and others v. Turkey*, App Nos. 41340/98, 41342/98, 41343/98, and 41344/98, Grand chamber judgment of February 13, 2003.
10. Mayer-Schönberger V., Cukier K. Big Data: a revolution that will transform how we live, work, and think. New York: Eamon Dolan/Houghton Mifflin Harcourt, 2013. 272 p.
11. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community OJ C [2007] 306/1.
12. Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. Judgment of the Court (Grand Chamber) of 13 May 2014, ECR [2014] 317 (hereinafter *Google Spain*).
13. Joined Cases C-293 & C-594/12, Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others, judgment of April 8, 2014, ECR [2014] I-238 (hereinafter Digital Rights Ireland).
14. Directive 2006/24/EC of the European Parliament and of the Council of March 15, 2006 on the retention of data generated or processed in connection with the provision of pub-licly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L [2006] 105/54.
15. C-362/14, Maximillian Schrems v. Data Protection Commissioner, judgment of October 6, 2015, ECLI:EU:C:2015:650 (hereinafter Schrems).
16. Commission Decision 2000/520/EC of July 26, 2000, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ [2000] L 215/7.
17. Cuijpers C., Purtova N., Kosta E. Data protection reform and the Internet: the Draft Data Protection Regulation. *Tilburg Law School Legal Studies Research Paper Series.* 2014. Vol. 3. 20 p.

Надійшла до редакції 26.11.2018

SUMMARY

Seryogin V. A. The reform of the European Union data protection framework: reasons and novations. The article highlights key changes that will result from the new General Data Protection Regulation (GDPR), which came into force in May 2018. An attempt was made to critically analyze this reform and evaluate some of its consequences, as well as an attempt to address them in the wider context of the digital economy and to manage it.

It was stated that data protection legislation in the EU went through an important reform. It is based on the three most important decisions of the Court of Justice of the European Union: on Google Spain, Digital Rights Ireland and Schrems.

The article is emphasized that the General Regulation contains a clear set of principles for data

processing; these include: a) legality, justice and transparency; b) restriction of purpose; c) minimizing data; d) accuracy; e) storage restrictions; e) integrity and confidentiality; is) accountability.

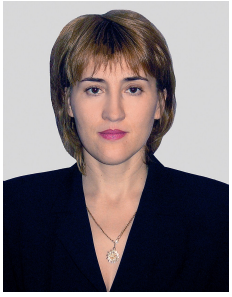
It is substantiated that the most significant changes provided by the General Regulations, which have a significant impact on the digital network environment in Europe, include: 1) greater protection provided to users and their personal data; 2) increased responsibility of the controllers and data processing entities; 3) a clearer understanding of the territorial boundaries of its action.

It is determined that the most acutely discussed change in the data protection legislation is the introduction in Art. 17 of the General Regulation "the right to be forgotten". A significant novelty is also the provision on portability of data, envisaging the right of users to receive their personal data in a structured, widely used and machine readable format.

GDPR frames a new obligation under the title of «data protection by design and by default». The controller is therewith obliged, while taking into account the state of the art; the cost of implementation; and the nature, scope, context, and purposes of processing, as well as the associated risks for rights and freedoms.

Keywords: *privacy, information privacy, personal data, personal data protection.*

УДК 341.48



Сироїд Т.Л.
доктор юридичних наук, професор
(Харківський національний університет імені В.Н. Каразіна)

DOI: 10.31733/2078-3566-2018-5-99-104

ЗАХИСТ ЖЕРТВ ТЕРОРИЗМУ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

Проаналізовано положення міжнародно-правових актів з протидії тероризму в аспекті захисту прав жертв злочину; акцентовано увагу на діяльності Організації Об'єднаних Націй, її спеціалізованих структур, уповноважених осіб та міжнародних регіональних організацій, зокрема, Організації з безпеки та співробітництва в Європі, Ради Європи, Європейського Союзу у цій сфері. Зроблено відповідні висновки.

Ключові слова: *жертви, захист, злочин, права людини, тероризм.*

Постановка проблеми. Питання протидії тероризму знаходиться в центрі уваги міжнародного співтовариства з 1934 року, коли Ліга Націй зробила перший крок в оголошенні цього явища поза законом, поставивши на обговорення проект Конвенції про запобігання і засудження тероризму 1937 р. (не набрала чинності). Лінію на протидію тероризму продовжила створена в 1945 р. Організація Об'єднаних Націй (далі – ООН), під егідою якої розроблено дев'ятнадцять універсальних документів по боротьбі з міжнародним тероризмом, що стосуються конкретних видів терористичної діяльності (станом на 2018 р.). Хоча в жодному з дев'ятнадцяти документів – конвенцій і протоколів по боротьбі з тероризмом не згадано окремо питання, пов'язані з правами та роллю жертв тероризму, в них підкреслено основоположну важливість включення державних принципів верховенства права, дотримання прав людини й основних свобод у складі національних законодавчих заходів та заходів кримінального судочинства щодо розслідування терористичних актів і судового переслідування за їх скоєння відповідно до міжнародних угод, стандартів і норм. Таким чином, права жертв опосередковано визнаються в цих документах як невід'ємний і важливий компонент ефективних заходів боротьби з тероризмом.

Знаменною подією стало прийняття у вересні 2006 р. державами-членами ООН Глобальної контртерористичної стратегії (A/RES/60/288), що є унікальним універсальним документом, направленим на зміцнення національних, регіональних та міжнародних зусиль у боротьбі з тероризмом. Уперше всі держави-члени погодилися із загальним стратегічним підходом до боротьби з тероризмом, не тільки пославши чіткий сигнал про те, що тероризм є неприйнятним в усіх його формах і проявах, але й висловивши рішучість зро-

© Сироїд Т.Л., 2018