ТЕОРЕТИКО-ПРАКТИЧНІ ПИТАННЯ РОЗВИТКУ ПРАВОВОЇ СИСТЕМИ УКРАЇНИ

THEORETICAL AND PRACTICAL ISSUES OF DEVELOPMENT OF THE LAW SYSTEM OF UKRAINE

https://doi.org/10.15407/econlaw.2022.01.045

УДК 342.7 + 347.121.2

Я.В. КОТЛЯРЕВСЬКИЙ, д-р екон. наук, проф., радник заступника Міністра фінансів України, м. Київ, Україна
orcid.org/0000-0003-3542-6952

М.В. СІРИК, канд. екон. наук, старш. викладач кафедри менеджменту підприємств, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна
orcid.org/0000-0002-0588-2183

М.О. ДЯЧЕНКО, координатор партнерської мережі «Освіта для сталого розвитку», експерт ПМГ ГЕФ-ПРООН, м. Київ, Україна
orcid.org/0000-0002-7518-3038

ПЕРСПЕКТИВНІ НАПРЯМИ УДОСКОНАЛЕННЯ РЕГУЛЮВАННЯ СФЕРИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

Ключові слова: персональні дані, регулювання, інституційне забезпечення, міжнародний досвід.

Досліджено стан захисту персональних даних в ЄС та Україні. Визначено вразливості регулювання щодо захисту персональних даних, проаналізовано європейський досвід, який можна використати в Україні. Розроблено рекомендації, що мають покращити нормативне та інституційне забезпечення подальшого розвитку сфери захисту персональних даних.

Вступ. Процес урегулювання питань, пов'язаних із захистом персональних даних, розпочався в Європейському Союзі із набранням чинності 13.12.1995 Директиви 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» (далі Директива), яка підлягала застосуванню до 2018 р. Директива за своєю природою не є законодавчим актом прямої дії, а її впровадження відбувається через ухвалення актів національного законодавства, спрямованих на досягнення визначених у Директиві цілей. Важливо, що країни — члени ЄС імплементували Директиву відповідно до власних правових традицій та культурних особливостей щодо приватності і захисту персональних даних. Як зазначала Європейська Комісія, унаслідок цього правове регулювання захисту персональних даних не було достатньо уніфікованим серед країн — членів ЄС [1]. Згодом, у грудні 2000 р., ухвалено Хартію ЄС про основні права, ст. 8 якої визначила захист персональних даних як право людини. Надалі принципи

Цитування: Котляревський Я.В., Сірик М.В., Дяченко М.О. Перспективні напрями удосконалення регулювання сфери захисту персональних даних в Україні. *Економіка та право*. 2022, № 1. С. 45—64. https://doi.org/10.15407/econlaw.2022.01.045

Хартії ЄС про основні права, що стосуються персональних даних, відображено в Лісабонській угоді від 01.12.2009, якою було внесено зміни до двох ключових актів ЄС: Угоди про ЄС і Угоди про заснування Європейської Спільноти. У результаті цього кожному у ЄС було гарантовано право на захист своїх персональних даних.

Аналіз останніх досліджень і публікацій. Уже у січні 2012 р. Європейська Комісія озвучила плани щодо уніфікації законодавства із захисту персональних даних. У ЄС шляхом ухвалення нового акта законодавства у сфері персональних даних Європейська Комісія визначила гармонізацію законодавства 27 країн — членів ЄС в один нормативно-правовий акт, удосконалення передачі корпоративних даних поза територією ЄС та посилення контролю приватних осіб над власними персональними даними [2]. У квітні 2016 р. в ЄС ухвалено Регламент Європейського Парламенту і Ради 2016/679/ЄС про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, застосування якого розпочалося 25.05.2018 (надалі Регламент).

Після ухвалення Регламенту з метою відображення на рівні національного законодавства стандартів захисту персональних даних, встановлених Регламентом, країни — члени ЄС або ухвалили нові законодавчі акти щодо захисту персональних даних, або внесли істотні зміни до актів законодавства, що діяли на момент ухвалення Регламенту. Окрім цього, відповідно до вимог Регламенту країни — члени ЄС повинні були проінформувати Європейську Комісію щодо положень національного законодавства, які стосуються: наглядового органу, відповідального за моніторинг дотримання Регламенту; санкцій, що підлягають застосуванню у випадку порушення Регламенту; узгодження права на захист персональних даних зі свободою на вираження поглядів та свободою інформації [3].

Регламент кардинально оновив способи збору та опрацювання персональних даних, до того ж не лише на території ЄС. Тому з метою дотримання відповідних вимог компанії як в ЄС, так і ті, хто ведуть свою діяльність на території ЄС або працюють зі споживачами з ринку ЄС, змушені оновлювати свої політики конфіденційності / персональних даних, закуповувати нове програмне забезпечення та оплачувати послуги правників. Утім, незважаючи на додаткові витрати корпоративного сектору, Регламент досягає важливих суспільних цілей, забезпечуючи громадянам ЄС найвищий рівень охорони та захисту прав на приватність.

Поряд із беззаперечними перевагами для захисту прав та інтересів громадян окремі експерти та дослідники наголошували, що головним недоліком Регламенту є його масштабність та складність. І природно, що оцінити інспіровані ним удосконалення щодо дотримання фундаментальних прав та справедливості можна буде лише під час реалізації відповідних положень у глобальному та національному вимірах, за результатами визначених періодів його використання на практиці [4].

З травня 2018 р. до березня 2021 р. національні органи контролю країн ЄС наклали приблизно 600 штрафів та санкцій на загальну суму понад 278,6 млн євро. Проте ці обсяги нерівномірно розподілено за країнами ЄС. Зокрема, найактивніший регулятор в Іспанії наклав понад 220 штрафних санкцій, водночас регулятори Словенії та Люксембургу не накладали за звітний період жодних штрафів. Хоча щодо останнього, вважаємо істотними елементи порівняльного аналізу деяких експертів, які обґрунтовано стверджують, що за бюджету у 5,7 млн євро національному регулятору Люксембургу вкрай важко розраховувати на успішні процесуальні та процедурні дії щодо відношення, наприклад, до корпорації *Amazon* як суб'єкта у сфері захисту персональних даних, адже такий обсяг фінансового ресурсу генерується в межах її комерційних операцій протягом 10 хвилин операційного часу [5]. Також кілька регуляторів спостерігають практику застосування процедурних схем подання скарг та/або зниження сум штрафів. Проте поки загальний обсяг штрафів зростає, великий обсяг заяв про порушення у сфері регулювання персональних даних залишається без належного реагування, особливо це стосується транскордонних справ і процесів. Зокрема, у цьому контексті національні регулятори європейських країн вбачають доцільною адаптацію таких операційних принципів у подальшій розбудові взаємодії та координації:

1) використання адекватних каналів та інструментів комунікації;

2) гармонізація та взаємна відповідність всіх національних процедур;

3) полегшення безпосередньої координації між інституціями;

4) чітке розмежування сфер відповідальності в ході координації [6].

Поряд з адміністративною складовою внутрішньоєвропейської координації, дедалі більшою мірою увагу регуляторів і дослідників привертає проблематика транскордонної передачі даних, що є іманентним для цифрового середовища аспектом. Навіть за наявності відповідних механізмів у Регламенті, зокрема передбачених ст. 3 та 5, що позиційно визначають, яким чином може відбуватися трансфер даних до третіх країн. Проте відповідні елементи не є вичерпними та утворюють інституційну невизначеність щодо вирішення цих питань конкретними регуляторами та в межах конкретних процесів і процедур [7].

Іншими помітними, проте достатньою мірою контроверсійними в контексті європейської практики регулювання сфери персональних даних є дослідницькі гіпотези в основі яких є твердження, що по відношенню до мультинаціональних корпорацій в частині накладання масштабних санкцій і штрафів (понад 1 млн євро) країни Західної Європи застосовують активніше відповідні положення порівняно з регуляторними інституціями країн Східної Європи [8].

В Україні відчутний прогрес у розвитку правового регулювання захисту персональних даних відбувся пізніше. Станом на 2010 р. суспільні відносини, що пов'язані із збиранням, зберіганням, використанням та поширенням інформації про особу, врегульовано у понад двох десятках неузгоджених між собою законів та підзаконних актів [9].

Мета статті: визначити перспективні напрями удосконалення сфери регулювання захисту персональних даних в Україні, а також ідентифікувати найрелевантніші підходи до формування відповідного інституційного забезпечення на основі дослідження аспектів суспільної практики, міжнародного досвіду, можливостей його гармонізації та адаптації до національного контексту.

Результати дослідження. З метою конкретизації та визначення механізмів реалізації положень ст. 32 Конституції України, якою проголошено право людини на невтручання в її особисте життя та встановлено заборону збирання, зберігання, використання поширення конфіденційної інформації про особу без її згоди, 01.06.2020 Верховною Радою України було ухвалено Закон України «Про захист персональних даних» (далі Закон), який набрав чинності з 01.01.2011. У січні 2014 р. наказом Уповноваженого Верховної Ради України з прав людини затверджено підзаконні акти для практичної імплементації Закону, зокрема:

- Типовий порядок оброблення персональних даних;
- Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних;
- Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про оброблення персональних даних, що становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних під час їхнього оброблення, а також оприлюднення вказаної інформації [10].

Відігравши важливу роль у законодавчій кодифікації правил опрацювання персональних даних, Закон, як і Директива, не встигав реагувати на технологічні зміни та викликані цим процеси у суспільстві, незважаючи навіть на багаторазові ітерації змін до тексту цього нормативно-правового акта. Водночас необхідність оновлення правового регулювання захисту персональних даних в Україні і його приведення до міжнародних стандартів захисту була очевидною протягом тривалого часу — і такий необхідний імпульс був наданий Угодою про Асоціацію між Україною та ЄС, зокрема згідно зі ст. 16 Україна та ЄС домовились співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів [11].

Безумовно, Регламент та Закон є нормативно-правовими актами, які доволі вагомо розрізняються між собою, що зумовлено як часом їхнього ухвалення, історичними передумовами, а також власне кількістю держав, для яких застосування цих законодавчих актів є обов'язковим. Порівняно з Законом Регламент урегульовує більший перелік питань, пов'язаних з обробленням персональних даних, має ширшу сферу застосування та глибшу деталізацію абсолютно усіх процесів та процедур щодо персональних даних.

Зазначимо, що Регламент застосовується екстериторіально, наповнений більшою кількістю понять, детальнішою регламентацією принципів оброблення персональних даних, прав, якими наділений суб'єкт персональних даних. На відміну від Закону Регламент прискіпливо визначає статус, права та обов'язки осіб, які обробляють персональні дані, вводить категорію посади «Офіцер із захисту даних», урегульовує питання транскордонного передавання даних, на детальнішому рівні визначає роль і завдання наглядового органу, відповідального за дотримання законодавства у сфері захисту персональних даних. Регламент присвячує більшу увагу питанням відповідальності за порушення персональних даних, диференціює санкції та чітко встановлює процедури їхнього накладення. Окрім цього, Регламент також містить певну кількість положень, які притаманні саме специфіці правової системи Європейського Союзу, наприклад, щодо співпраці контрольних органів країн — членів ЄС з питань захисту персональних даних у межах ЄС або звітів Європейської Комісії до Європейського Парламенту та Ради щодо оцінювання та перевірки виконання Регламенту.

Водночас норми Закону характеризуються переважанням радше загальних вимог стосовно захисту персональних даних без достатнього рівня їхньої деталізації, що створює значні труднощі під час практичного застосування. Тоді як частина питань щодо опрацювання персональних даних врегульовується лише загальним чином, деякі питання взагалі не становлять предмет регулювання Закону, зокрема, питання, пов'язані з інтернет-маркетингом, транскордонною передачею даних тощо. Окремою контроверсійною характеристикою Закону є труднощі, пов'язані із належним забезпеченням контролю за його дотриманням: Уповноважений Верховної Ради України з прав людини, окрім здійснення контролю за дотриманням законодавства про захист персональних даних, також виконує й ряд інших визначених законодавством завдань. Унаслідок цього контрольна функція у сфері захисту персональних даних не забезпечена достатньою інституційною спроможністю, зокрема людськими ресурсами та експертизою, що безумовно негативно впливає на стан дотримання законодавства у сфері персональних даних в Україні [12]. Детальніший огляд спільних та відмінних положень Закону та Регламенту у розрізі окремих правових категорій наводиться у табл. 1.

Оскільки Закон характеризується меншою кількістю вимог і зобов'язань для осіб, що здійснюють опрацювання персональних даних, дотримання законодавства для бізнесу в Україні є менш обтяжливим. Однак фізичним особам в Україні в контексті захисту їхніх інтересів надано менший обсяг прав, що стосуються персональних даних. Окрім того, реалізація таких прав не регламентована належно. Резиденти України позбавлені гарантій захисту своїх персональних даних, що надані резидентам ЄС, зокрема, зазначені вразливості можна відстежити за їхніми проявами на основі національної судово-юридичної практики, що ґрунтується на аналізі звітної документації уповноважених органів, даних Єдиного Реєстру Судових Рішень, релевантних публікацій у ЗМІ.

Зараз в Україні захистом персональних даних опікується лише Уповноважений Верховної Ради з прав людини та кіберполіція. Уповноважений може скласти адміністративний протокол на державний орган чи установу, якщо вони порушують право людини на захист персональних даних, а кіберполіція розслідує кримінальні правопорушення, зокрема, пов'язані з витоком даних із держреєстрів. За інформацією з Єдиного порталу судових рішень, у 2019—2020 рр. нараховано лише 15 вироків за такими справами. За минулі роки таких справ ще менше [13]. Провести детальніший аналіз судових рішень за кримінальними справами немає можливості, оскільки вказані судові рішення, як правило, є з обмеженим доступом.

За даними Департаменту кіберполіції, упродовж 2018 р. поліцейські виявили 6 тис. злочинів, вчинених у сфері використання високих інформаційних технологій, 7 % із них — продаж та аналізування викрадених баз даних. Також омбудсменом проведено 36 перевірок розпорядників персональних даних і складено 26 приписів про усунення порушень [14].

Як зазначається у щорічному звіті, омбудсмен загалом розглянув майже удвічі більше повідомлень про порушення права на захист персональних даних — 2031 у 2020 р. проти 1061 у 2019 р. [14, 15]. Водночас складено і на-

Таблиця 1. **Систематизація порівняльних особливостей регулювання сфери захисту персональних даних у Україні та ЄС**

№ з/п	Напрям порівняння та його загальна характеристика	Порівняльні особливості Закону	Порівняльні особливості Регламенту
1	**Матеріальна та територіальна дія.** Матеріальна сфера дії Закону та Регламенту не відрізняється, натомість територіальна дія обох законодавчих актів не є ідентичною	Поширюється на діяльність з оброблення персональних даних, що здійснюється із застосуванням автоматизованих засобів, чи призначені до внесення до картотеки без застосування таких засобів. Містить перелік випадків, коли нормативно-правові акти не підлягають застосуванню. Обидва акти не застосовуються, якщо оброблення здійснюється фізичною особою виняткова для особистих чи побутових потреб. Українські стандарти захисту персональних даних також спростовують застосування Закону, якщо оброблення здійснюється виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів. Закон поширює свою дію лише на територію України	Поширюється на діяльність з оброблення персональних даних, що здійснюється із застосуванням автоматизованих засобів чи призначені до внесення до картотеки без застосування таких засобів. Містить перелік випадків, коли нормативно-правові акти не підлягають застосуванню. Обидва акти не застосовуються, якщо оброблення здійснюється фізичною особою виняткова для особистих чи побутових потреб. Регламент охоплює також діяльність з оброблення персональних даних не лише щодо резидентів ЄС, а й щодо резидентів інших країн, якщо опрацювання персональних даних пов'язано з пропонуванням товарів і послуг суб'єктам даних з ЄС або у випадку моніторингом поведінки суб'єктів даних в ЄС . Отже, компанії, що здійснюють дослідження суб'єктів ринку ЄС, використовують персональні дані громадян ЄС для розроблення власних продуктів або ведуть будь-яку діяльність у ЄС, повинні також дотримуватися вимог Регламенту
2	**Категоріально-термінологічна база.** Ширший предмет регулювання та новітнішій підхід до регламентації питань, пов'язаних з обробленням персональних даних, зумовив надання Регламентом більш ніж удвічі більшої кількості визначень, які застосовуються у ньому, порівняно із Законом. Менша кількість понять у Законі не лише свідчить про вужчий предмет його регулювання, а й має безпосередні практичні наслідки для його застосування. Відсутність значної кількості понять, що містяться у Регламенті, має прямий негативний вплив на передбачуваність та чіткість регулювання в Україні та, відповідно, якість гарантування та забезпечення прав суб'єктів персональних даних	Закон надає визначення 11 поняттям, зокрема «база персональних даних», «володілець персональних даних», «згода суб'єкта персональних даних», «знеособлення персональних даних», «картотека», «оброблення персональних даних», «одержувач», «персональні дані», «розпорядник персональних даних», «суб'єкт персональних даних» і «третя особа»	Регламент має 26 визначень та охоплює додатково такі категорії як «обмеження оброблення персональних даних», «профілювання», «псевдомінізація», «файлова система», «контролер», «процесор», «витік персональних даних», «генетичні дані», «біометричні дані», «дані щодо здоров'я», «місце заснування», «представник», «підприємство», «група підприємств», «обов'язкові корпоративні правила», «наглядовий орган», «відповідний наглядовий орган», «транскордонна обробка», «послуга інформаційному суспільству» та «міжнародна організація»

Продовження табл. 1

№ з/п	Напрям порівняння та його загальна характеристика	Порівняльні особливості Закону	Порівняльні особливості Регламенту
3	**Регламентація принципів оброблення персональних даних.** Відсутність чіткої регламентації засад опрацювання персональних даних в Законі призводить до непередбачуваного, нечіткого та некоректного застосування положень українського законодавства у сфері персональних даних, що має безпосередній вплив на здатність забезпечення належного рівня захисту, який надається суб'єктам персональних даних. За рахунок детального визначення принципів оброблення персональних даних на рівні Регламенту, європейські стандарти захисту персональних даних містять менше невизначених або непередбачуваних положень, що спрощує правозастосування та сприяє належному забезпеченню прав суб'єктів даних у ЄС	Закон взагалі не визначає окремо принципи оброблення персональних даних та не розкриває їхню суть. Опосередковано зміст принципів можна виокремити у положеннях ст. 6 Закону, яка встановлює вимоги щодо цільового призначення, правомірності і прозорості оброблення персональних даних, їхньої точності і достовірності, а також адекватності та ненадмірності. Окрім цього, згідно з вимогами Закону персональні дані повинні оброблятися у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися. Закон лише на загальному рівні надає уявлення про зміст згоди на опрацювання персональних даних, не встановлює заборону на згоду за замовчуванням, не передбачає можливості відкликати згоду в будь-який момент та не встановлює обмеження щодо віку, з якого з'являється можливість надання дозволу на оброблення персональних даних	На рівні Регламенту принципам присвячено сім статей, в яких принципи оброблення персональних даних регламентовано на доволі детальному рівні: «Законність, правомірність і прозорість». За своєю суттю цей принцип вимагає від особи, що збирає персональні дані, надання чітких пояснень, для чого збираються персональні дані суб'єкта та яким чином вони будуть використовуватися. «Цільове обмеження». Опрацювання персональних даних має бути спрямоване для явних та законних цілей. Компанії не повинні збирати дані, які не відповідають визначеній меті. «Мінімізація даних». Дані мають бути адекватними, відповідними (до мети оброблення) та обмежуватись виключно тими цілями, з метою досягнення яких вони опрацьовуються. Компанії повинні бути переконаними, що вони не акумулюють надлишкові дані та зберігають мінімальний обсяг даних про особу, необхідних для їхнього використання. «Точність». За цим принципом, дані, що опрацьовуються, повинні залишатися точними та дійсними для цілей опрацювання. Неточні персональні дані має бути стерто чи виправлено без затримки. «Обмеження зберігання». Цей принцип вимагає, аби дані зберігалися у формі, що дає змогу ідентифікувати суб'єкта даних, але не довше, ніж це є необхідним для цілей оброблення. «Цілісність і конфіденційність». Дані обробляються так, що забезпечують належну безпеку персональних даних, зокрема захист проти несанкціонованого чи незаконного опрацювання та проти ненавмисної втрати, знищення чи завдання шкоди. Компанія, яка збирає та опрацьовує персональні дані, несе повну відповідальність за здійснення щодо них заходів безпеки. Регламент на детальному рівні перелічує випадки, коли опрацювання даних є законним та встановлює ключові вимоги щодо надання згоди суб'єкта даних на оброблення його персональних даних. Так, контролер повинен мати здатність продемонструвати згоду суб'єкта даних, яка має здійснюватися у зрозумілій та доступній формі, з використанням чітких і простих формулювань. Здебільшого Регламентом врегульовано питання умов, що застосовуються до згоди дитини в сфері послуг інформаційного суспільства: згода дитини без потреби залучити опікуна є законною у разі, якщо така дитина досягла віку 16 років

Продовження табл. 1

№ з/п	Напрям порівняння та його загальна характеристика	Порівняльні особливості Закону	Порівняльні особливості Регламенту
4	**Класифікація персональних даних.** Обидва нормативно-правові акти застосовують до спеціальних особових (чутливих) даних жорсткіші вимоги стосовно процедури їхнього оброблення, збирання, зберігання та передачі третім особам	Врегулювання Законом питань стосовно особливостей оброблення спеціальних особових (чутливих) даних відрізняється менш чіткою та невичерпною логікою	Регламент відносить до спеціальних особових (чутливих) даних ширший перелік даних, включно з психометричними даними та даними, що стосуються сексуальної орієнтації. Регламент містить ширший перелік винятків, коли обробка спеціальних особових (чутливих) даних допускається. До такого переліку входять, серед іншого, випадки, коли суб'єкт персональних даних неспроможний надати згоду, а оброблення є необхідним для захисту його життєво важливих інтересів. Опрацювання спеціальних особових (чутливих) даних дозволяється також, якщо воно стосується даних, які суб'єкт персональних даних явно оприлюднив, або якщо обробка необхідна в цілях архівування в суспільних інтересах, цілях наукового чи історичного дослідження або статистичних цілях, що здійснюється на підставі закону тощо
5	**Права суб'єктів персональних даних.** Як Законом, так і Регламентом суб'єкти даних наділені правом на захист від рішення, що ґрунтується винятково на автоматизованому опрацюванні, яке має для нього правові наслідки, проте за змістом і деталізацією права суб'єктів відрізняються докорінно	У Законі такі права суб'єктів персональних даних перелічені одним реченням у відповідних частинах ст. 8: суб'єкт даних має право на інформацію про персональні дані, що охоплює інформацію про умови надання доступу до них, джерела збирання, їхнього місцезнаходження, мету оброблення, перебування володільця чи розпорядника, а також доступ до них. Законом не наділено суб'єкта даних правом обмежити опрацювання його даних контролером, тоді як Регламент передбачає, що таке право може бути реалізоване у випадку виникнення обставин, коли опрацювання даних є незаконним і суб'єкт надсилає запит щодо обмеження їхнього використання замість знищення, або контролеру більше не потрібні персональні дані для цілей опрацювання, але їх вимагає суб'єкт даних для формування чи здійснення правових вимог. Хоча «право бути забутим» та право на обмеження опрацювання даних у Законі	Регламент присвячує цьому питанню окремий розділ та 12 статей із детальним розкриттям змісту й суті кожного з прав та відповідних кореспондувальних обов'язків, а також способів та особливостей їхньої реалізації. Окрім цього, певні права, надані суб'єктам даних у ЄС згідно з Регламентом, взагалі не передбачені для українських суб'єктів персональних даних. Для цілей забезпечення реалізації права на інформацію Регламент розширює перелік інформації, що надається суб'єкту даних. Серед іншого, суб'єкт персональних даних у ЄС має право отримати інформацію про особу та контактні дані контролера (представника контролера), контактні дані співробітника з питань захисту даних, законодавчу базу для опрацювання, одержувача чи категорії одержувачів персональних даних, намір передати персональні дані до третьої країни чи міжнародної організації, період зберігання, можливість відкликання згоди на оброблення персональних даних та подання скарги до наглядового органу тощо . Окрім цього, для цілей реалізації права на доступ Регламентом покладено на контролера обов'язок надавати підтвердження суб'єкту персональних даних про сам факт опрацювання його даних. Регламентом також детально регламентовано реалізацію суб'єктом даних групи прав, що стосується виправлення та видалення персональних даних. До таких прав належить, зокрема, право на виправлення неточних персональних даних без будь-якої необґрунтованої затримки, що частково перегукується з визначеним у Законі правом суб'єкта даних пред'явити вмотивовану вимогу щодо зміни персональних даних, якщо ці дані є недостовірними.

Продовження табл. 1

№ з/п	Напрям порівняння та його загальна характеристика	Порівняльні особливості Закону	Порівняльні особливості Регламенту
		належно не регламентовані, Закон все ж наділяє суб'єкта даних правом пред'являти вмотивовану вимогу (1) щодо знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно (2) володільцю персональних даних із запереченням проти оброблення своїх персональних даних. Проте такі норми не можуть замінити детальну регламентацію «права бути забутим», як це врегульовано Регламентом. На сьогодні фактично єдиним доступним способом видалення даних щодо особи є набрання законної сили рішення суду щодо їхнього видалення або знищення. В Україні обмеження прав суб'єктів даних допускається у випадках, передбачених законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб	Окремою новелою Регламенту є закріплення та регламентація особливостей реалізації «права бути забутим», тобто знищення персональних даних, яке повинен здійснити контролер без будь-якої безпідставної затримки. Також передбачено надання суб'єкту даних права отримувати на підставі запиту інформацію про будь-яке виправлення чи знищення персональних даних, а також регламентація питань, пов'язаних з мобільністю даних. Регламент передбачає ширший перелік випадків, коли може бути здійснене обмеження прав суб'єктів даних, розширеним є перелік таких випадків та окремо зазначається про можливість обмеження прав для цілей оборони, громадської безпеки, запобігання, розслідування, виявлення або переслідування за скоєння злочинів або для виконання кримінальних покарань, інших важливих цілей загального суспільного інтересу ЄС або країни-члена, а також захисту незалежності судових органів і судових процесів
6	**Статус, обов'язки та відповідальність суб'єктів оброблення персональних даних права.** Однією з ключових відмінностей Закону і Регламенту є ступінь деталізації прав, обов'язків, відповідальності та вимог до осіб, що здійснюють опрацювання персональних даних. Загалом з метою забезпечення належного захисту персональних даних Регламент, на відміну від Закону, на детальному рівні визначає обов'язки, відповідальність та вимоги щодо оброблення персональних даних усіма особами, залученими до таких процедур	Володілець персональних даних визначає мету оброблення персональних даних, встановлює склад цих даних та процедури їхнього оброблення. Розпорядником персональних даних є особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця. На жаль, комплексно їхні права, обов'язки, відповідальність, а також формати взаємодії між собою, жорсткі вимоги до опрацювання даних не врегульовано Законом. Категорії «представник розпорядника /	Згідно з Регламентом особами, що обробляють персональні дані, є контролер (*data controller*) та оператор (*data processor*) відповідно. Контролер виконує керівну функцію над оператором, а саме вказує останньому на порядок та правильність оброблення персональних даних. Оператор же виконує функцію виконавця, тобто здійснює процедури, необхідні для збереження персональних даних. Регламентом покладено на контролерів загальний обов'язок вживати належних технічних та організаційних заходів для забезпечення оброблення даних відповідно до вимог Регламенту та перелічено, якими ці заходи можуть бути. Бізнес-процеси контролера та оператора, відповідно до яких опрацьовуються персональні дані, повинні бути побудовані за принципом «приватність за призначенням і за замовчуванням», тобто з використанням псевдонімів чи повної анонімізації, налаштувань найвищого рівня приватності

Продовження табл. 1

№ з/п	Напрям порівняння та його загальна характеристика	Порівняльні особливості Закону	Порівняльні особливості Регламенту
		володільця даних», «спільний розпорядник даних» відсутні у Законі. На рівні Закону визначено, що володілець персональних даних може доручити оброблення персональних даних розпоряднику персональних даних відповідно до договору, укладеного в письмовій формі, проте зміст такого договору не визначено. Відповідно до українських стандартів захисту персональних даних на розпорядника даних Законом не покладено обов'язку проводити оцінювання впливу операцій опрацювання даних на захист персональних даних	за замовчуванням, щоб дані не були доступні публічно без згоди та не могли бути використані для ідентифікації суб'єкта без додаткової інформації, що зберігається окремо. Тягар доведення відповідності технічних і організаційних заходів Регламенту покладено на контролера. У разі, якщо передача даних здійснюється поза територією ЄС, контролер або оператор повинен призначити в письмовій формі представника в ЄС, який отримує відповідний мандат, що дозволяє наглядовим органам та суб'єктам даних звертатися до нього замість контролера або оператора з усіх питань, пов'язаних з опрацюванням даних. Особливим чином врегульовує Регламент і питання взаємозв'язків та взаємних зобов'язань між контролером та оператором: положення Регламенту безпосередньо визначають зміст договору щодо обробки даних між контролером і оператором, включно зі встановленням зобов'язання оператора і залучених до оброблення субоператорів також перевіряти вказівки контролера. Статтею 30 Регламенту встановлено обов'язки кожного контролера і за необхідності, представника контролера вести запис опрацювання даних, що належать до його сфери відповідальності, визначено безпосередній перелік інформації, що повинен міститися у таких записах. Окрім цього, на контролера і оператора накладено певні нові зобов'язання щодо дій у разі настання події витоку даних, зокрема, повідомити відповідні органи влади та суб'єктів даних, для яких встановлені короткі строки виконання. Регламентом на контролера даних також покладено обов'язок провести оцінювання впливу операцій опрацювання на захист персональних даних, якщо тип опрацювання, зокрема з використанням нових технологій, і з урахуванням специфіки, обсягу, контексту і цілей опрацювання, імовірно може призвести до виникнення високого ризику для прав і свобод фізичних осіб. Регламент в окремих випадках вимагає від контролера і оператора призначення на підставі професійних якостей і зокрема, експертних знань із права та практики захисту даних Офіцера із захисту даних. Така вимога є обов'язковою, серед іншого, якщо опрацювання здійснює публічний орган або установа (за винятком судів), або основні види діяльності контролера або оператора становлять операції опрацювання, які, в силу їхньої специфіки, обсягів або цілей, вимагають регулярного, систематичного і широкомасштабного моніторингу суб'єктів даних

Продовження табл. 1

№ з/п	Напрям порівняння та його загальна характеристика	Порівняльні особливості Закону	Порівняльні особливості Регламенту
7	**Урегулювання питань транскордонної передачі персональних даних.** На відміну від Регламенту, Закон повністю оминає врегулювання питань, пов'язаних з транскордонною передачею даних, шляхом встановлення інструментів та правових підстав для передачі даних поза межами території регулювання	Закон не містить відповідних положень, тож питання передачі персональних даних поза територією України є неврегульованим	За загальним принципом передавання персональних даних до третьої країни чи міжнародної організації може відбуватися лише тоді, коли контролер та оператор дотримуються умов, передбачених Регламентом. Передавання персональних даних до третьої країни чи міжнародної організації може відбуватися, якщо Європейська Комісія у формі імплементаційного акта вирішила, що третя країна, територія або відповідна міжнародна організація забезпечує належний рівень захисту. Перед ухваленням рішення про відповідність Європейська Комісія оцінює фактори, прямо визначені Регламентом, а саме: верховенство права, повагу до прав людини та фундаментальних свобод, законодавство, зокрема щодо громадської безпеки, оборони, національної безпеки та кримінального права і доступу органів публічної влади до персональних даних, а також його імплементацію і судову практику; дієве функціонування незалежних наглядових органів із відповідальністю за забезпечення та дотримання норм про захист даних, зокрема й належними правозастосовними повноваженнями; міжнародні зобов'язання, що взяли на себе третя країна або відповідна міжнародна організація. Щодо передачі даних з урахуванням належних гарантій, контролер або оператор може надати, зокрема, типові договірні положення, обов'язкові корпоративні правила, сертифікацію, кодекси поведінки для отримання персональних даних. Насамкінець іншими правовими підставами для транскордонної передачі даних можуть, серед іншого, бути явна згода із зазначенням можливих ризиків щодо передачі даних чи переслідування суспільного інтересу або життєво важливого інтересу фізичної особи
8	**Статус, повноваження, інституційна спроможність наглядових органів, відповідальних за дотримання законодавства у сфері персональних даних.** Регламент та Закон на різних рівнях деталізації визначають роль наглядових органів, відповідальних за дотримання законодавства у сфері захисту персональних даних, проте українська модель наглядового органу у сфері персональних даних	У Законі регламентовано повноваження Уповноваженого Верховної Ради України з прав людини як органу, що здійснює контроль за додержанням законодавства про захист персональних даних, зокрема, ухвалювати рішення за результатами розгляду скарг та звернень з питань захисту персональних даних, проводити перевірки та видавати приписи, отримувати доступ до	Регламент підходить до питання наглядового органу комплексніше, поряд з його повноваженням визначає його завдання, гарантії незалежності та інституційної спроможності. Регламент також дозволяє покладати відповідальність за моніторинг застосування Регламенту на один чи декілька органів. Щодо завдань наглядового органу, то вони охоплюють підвищення обізнаності громадськості та контролерів і операторів щодо опрацювання персональних даних, консультування інших органів влади щодо правових та адміністративних інструментів, пов'язаних з опрацюванням персональних даних, розгляд скарг, співпрацю з іншими наглядовими

Продовження табл. 1

№ з/п	Напрям порівняння та його загальна характеристика	Порівняльні особливості Закону	Порівняльні особливості Регламенту
	апріорі значно поступається у можливостях та спроможності з огляду на окреслені порівняльні особливості	інформації, затверджувати нормативно-правові акти, надавати рекомендації щодо практичного застосування законодавства про захист персональних даних тощо	органами для забезпечення послідовності застосування та забезпечення виконання Регламенту, ухвалення зобов'язальних корпоративних правил та заохочення щодо розроблення кодексів поведінки. Для виконання вказаних завдань наглядовий орган наділяється слідчими та виправними повноваженнями. Слідчі повноваження включають розпорядження контролеру або оператору надати будь-яку інформацію, яку наглядовий орган потребує для виконання своїх завдань, проведення розслідувань у формі перевірок захисту даних, здійснення перегляду сертифікацій, отримання доступу до будь-яких приміщень контролера або оператора, у тому числі до будь-якого обладнання і засобів опрацювання даних. Серед виправних повноважень, якими наділяються відповідні наглядові органи, зокрема, є надсилання попередження контролеру або оператору про те, що призначені операції опрацювання ймовірно порушать положення Регламенту, винесення доган, наказів дотримуватися запитів суб'єкта даних, привести операції опрацювання у відповідність з положеннями Регламенту, повідомити суб'єкта даних про порушення захисту персональних даних, здійснити виправлення чи стирання персональних даних або обмеження опрацювання, а також відкликання сертифікації, накладення адміністративних штрафів тощо. Регламент приділяє значну увагу питанням забезпечення незалежності та інституційної спроможності наглядового органу, без чого ефективна реалізація наведених завдань і повноважень є неможливою. Так, наглядовий орган повинен залишатися вільним від зовнішнього впливу та не повинен запитувати, чи приймати вказівки від будь-якої особи. Незалежність наглядового органу забезпечується за рахунок прозорих процедур призначення його членів, встановлення вимог до їхньої компетентності, строковістю перебування на посаді та передбаченням запобіжників щодо конфліктів інтересів. Для забезпечення інституційної спроможності наглядового органу Регламент передбачає такі гарантії: забезпеченість достатніми людськими, технічними та фінансовими ресурсами, приміщеннями та інфраструктурою, необхідними для виконання завдань та обов'язків; свобода у виборі власного персоналу, який буде підпорядковуватися лише наглядовому органу;

Продовження табл. 1

№ з/п	Напрям порівняння та його загальна характеристика	Порівняльні особливості Закону	Порівняльні особливості Регламенту
			наявність власного публічного бюджету, що може бути частиною загальнодержавного або національного бюджету. Окрім цього, Регламентом утворюється Європейська рада із захисту даних як орган ЄС, що має правосуб'єктність. Її головним завданням є забезпечення послідовності застосування Регламенту, і для цих цілей Європейська рада із захисту даних, зокрема, консультує Європейську Комісію з будь-якого питання, пов'язаного із захистом персональних даних у ЄС, видає настанови, рекомендації та інформацію про кращі практики у сфері персональних даних для контролерів, процесорів і приватних осіб, сприяє ефективній співпраці між усіма наглядовими органами в ЄС тощо
9	**Відповідальність за порушення у сфері обробки персональних даних.** Ефективна практика правозастосування у сфері захисту персональних даних потребує якісного врегулювання питань, пов'язаних із настанням відповідальності за вчинення правопорушень. На відміну від Регламенту, модель притягнення до відповідальності за порушення у сфері захисту персональних даних в Україні поряд з недостатньою інституційною спроможністю наглядового органу не виконують стримувальну функцію для запобігання правопорушенням та не дають змоги відновити справедливість у випадку порушень прав суб'єктів персональних даних	Закон приділяє питанням відповідальності за порушення законодавства про захист персональних даних лише одне речення, зазначаючи, що такі порушення тягнуть за собою відповідальність, встановлену законом, відсилаючи такдо інших актів законодавства, якими встановлена відповідальність. У рамках українського правового поля діяння, які становлять порушення у сфері захисту персональних даних, а також відповідні санкції перелічені у статті 188-39 Кодексу України про адміністративні правопорушення. Так, до таких порушень відноситься, зокрема: неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про оброблення персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей; невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини	Регламент присвячує питанням відповідальності окремий розділ. Так, суб'єкти даних наділені правом подання скарги будь-якому наглядовому органу в межах країн — членів ЄС, якщо вони вважають, що їхні права було порушено у результаті опрацювання персональних даних. Регламентом також встановлені гарантії дієвого судового захисту проти наглядового органу та контролера і оператора. Принциповим положенням Регламенту є запровадження загального правила, згідно з яким кожен контролер або оператор несе відповідальність за усю шкоду, заподіяну з їхньої вини. Штраф за порушення Регламенту може досягати 20 млн євро або 4 % від світового обороту порушника. Суб'єкт даних може одночасно звернутись як до оператора, так і до контролера для отримання компенсації. Під час визначення санкцій за порушення прав щодо персональних даних враховуються чинники, серед яких: специфіка порушення, характер вини порушення, дії, вжиті контролером або оператором для зниження рівня шкоди, заподіяної суб'єктами даних, ступінь відповідальності контролера або оператора, будь-які належні попередні порушення з боку контролера або оператора, рівень співпраці з наглядовим органом для відшкодування порушення і скорочення можливих негативних наслідків порушення тощо

Закінчення табл. 1

№ з/п	Напрям порівняння та його загальна характеристика	Порівняльні особливості Закону	Порівняльні особливості Регламенту
		або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних; недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних. Санкції за вчинення наведених вище правопорушень передбачені у формі штрафу, найбільший розмір якого не перевищує 34 000 грн	

правлено до суду менше на один протокол про адміністративне правопорушення за ч. 4 ст. 188-39 Кодексу про адміністративні правопорушення України (далі КУАП) (порушення законодавства у сфері захисту персональних даних) — дев'ять 2020 р. проти десяти 2019 р. Найбільше такі порушення фіксувалися у сферах фінансових і банківських послуг, страхування, житлово-комунальних послуг, охорони здоров'я соціального захисту, освіти, а також у процесі оброблення персональних даних під час здійснення відеоспостереження, обліку адміністративних і кримінальних правопорушень [14]. Наявність 9—10 протоколів означає, що для повноцінного захисту персональних даних громадян України можливостей омбудсмена зовсім недостатньо, адже у відділі перевірок працює лише п'ять осіб, а загалом відповідний департамент налічує 22 працівники. Цього недостатньо для належного контролю. Додатково існує ще й законодавча обмеженість — омбудсмен не може самостійно притягнути винних осіб до відповідальності, тільки у судовому порядку.

2019 р. у зв'язку з продовженням реформи децентралізації в Україні та активним утворенням об'єднаних територіальних громад постало питання забезпечення органами місцевого самоврядування дотримання прав і свобод людини і громадянина, зокрема питання забезпечення захисту права особи на приватність. Тому одним із Стратегічних напрямів діяльності Уповноваженого було здійснення моніторингу дотримання прав людини у сфері захисту персональних даних під час ведення та адміністрування органами місцевого самоврядування реєстрів об'єднаних територіальних громад. За результатами перевірок 16 виконавчих органів сільської, селищної, міської ради та центрів надання адміністративних послуг виявлено низку системних порушень щодо реалізації права особи на приватність, у зв'язку із чим Уповноваженим 2020 р. підготовлено Рекомендації щодо застосування законодавства про захист персональних даних для органів реєстрації (виконавчих органів сільської, селищної або міської ради, центрів надання адміністративних послуг) [16].

Також у другій половині 2019 р. Уповноваженим розпочато перевірки дотримання права на приватність під час функціонування електронної системи охорони здоров'я та комп-

лексної системи відеоспостереження м. Києва, за результатами яких видано три приписи та надано рекомендації в дев'ятьох актах реагування щодо належного виконання вимог законодавства у сфері захисту персональних даних [14].

Проте судових рішень, відповідно до яких було б встановлено матеріальну, адміністративну та/або іншу відповідальність за порушення права на захист персональних даних у вітчизняній судовій практиці, майже немає. Здебільшого йдеться про усунення порушення.

Так, Верховний Суд України встановив порушення прав співробітника Чопської міськради на захист персональних даних. У березні 2015 р. особисте фото було опубліковано в одній із місцевих газет «з особою чоловічої статі» без відповідного дозволу. Суд підтвердив рішення першої інстанції, яким визнав, що публікація цього фото стосується особистого життя чиновниці та не несе жодної ролі для суспільства, а отже, не могло бути опубліковано без її згоди.

У березні 2019 р. Верховний Суд скасував рішення попередніх інстанцій і відправив на новий розгляд справу щодо відеоспостереження. Зокрема, позивач скаржився на те, що його сусід добудував прибудову до свого будинку і встановив чотири камери, дві з яких направлені в бік його ділянки, що є порушенням права на приватне життя. Нижчі інстанції ухвалили рішення, вказавши, що позивач не надав достатніх доказів. Утім, касація встановила порушення під час розгляду цієї справи і відправила її на новий розгляд [17].

Львівський окружний адміністративний суд у січні 2018 р. визнав порушення прав позивача і зобов'язав Міністерство внутрішніх справ видалити з баз даних інформацію про повідомлення йому три роки до того про підозру у кримінальному правопорушенні, оскільки інший суд закрив це провадження. Суд визнав, що після закриття справи зберігання цієї інформації є втручанням в його право на повагу до приватного життя, що не відповідає критерію «згідно із законом» [18].

Єдиний реєстр судових рішень містить також чимало скарг до омбудсмена щодо неналежного розгляду заяви про порушення прав людини. Так, одна з них стосувалася оприлюднення особою на її сторінці в одній із соціальних мереж запиту на доступ до публічної інформації, що містив персональні дані позивача. Суд залишив заяву без руху, даючи позивачу можливість виправити допущені помилки у скарзі [19].

Також украй мало судових рішень щодо предметного розгляду справ про витоки інформації з баз персональних даних. Наприклад, до штрафу в 17 000 грн засудили раніше неодноразово судиму громадянку України, яка через месенджер продавала «базу мешканців України», яка містила ПІБ, адреси, паспортні дані, ІПН та іншу інформацію [20].

За підсумками 2019 р. Офіс омбудсмена повідомив про передачу однією навчальною установою персональних даних (прізвища, імена, номери телефонів, електронні адреси, *IP*-адреси, регіон, дата та час входу, а також за наявності посади, назви компаній, профілі в соціальних мережах та фото) адвокатів, помічників адвокатів, стажистів адвокатів, а також інших осіб без їхнього відома та однозначної згоди. Під час перевірки було встановлено, що фактично здійснювалося оброблення персональних даних користувачів онлайнових курсів в електронному вигляді за допомогою онлайнової платформи, хостинг якої фізично розташований на території інших юрисдикцій. 2019 р. Подільський районний суд Києва закрив це провадження, не побачивши складу адміністративного правопорушення. Зокрема, посилаючись на позицію відповідача, що представники омбудсмена не аналізували програмний код сайту, а тому не довели самого факту несанкціонованої передачі даних [21].

Також 2019 р. один із депутатів Черкаської міської ради VIII скликання за депутатським запитом отримав від Черкаської міської ради Будівельний паспорт одного з об'єктів будівництва, який містив персональні дані власника, та виклав його у вільному доступі на вебсторінці у соціальній мережі. Це призвело до незаконного доступу до них невстановленого кола осіб та безпідставного втручання у приватне життя. Постановою Соснівського районного суду м. Черкаси від 04.07.2019 порушника було притягнуто до адміністративної відповідальності та стягнуто штраф у розмірі 3400 грн. Проте питання про видалення цієї інформації не вирішувалося і не могло бути

вирішеним у межах провадження у справах про адміністративні правопорушення. Водночас практика застосування законодавства про захист персональних даних інколи є достатньо контроверсійною та нетривіальною. Наприклад, використовуються окремі аспекти регулювання захисту персональних даних як підстава для оскарження чинності господарських договорів, як підстава для скасування (зупинення дії) регуляторних актів (справа щодо «функціонування ринку природного газу»), для уникнення виконання обов'язку оприлюднення документів [13].

Дещо цікавішою є практика Європейського суду з прав людини (ЄСПЛ) щодо порушення права на захист персональних даних роботодавцем. У рішенні «Суріков проти України» (2017) суд зазначив, що роботодавець заявника довільно збирав, зберігав та використовував дані стосовно його психічного здоров'я у зв'язку із заявою останнього про підвищення, а також відкрив ці дані колегам заявника та суду під час відкритого розгляду справи. ЄСПЛ вказав, що це непропорційне втручання у право заявника, що не було необхідним у демократичному суспільстві, тому вважається порушенням [22].

Зазначене є свідченням нагальної потреби удосконалення вітчизняної сфери регулювання захисту персональних даних, а також використання у цьому контексті найадекватніших європейських стандартів, їхньої гармонізації та адаптації до національного контексту із урахуванням придатності для найуразливіших аспектів захисту інтересів приватності й безпеки особистості, зокрема у добу технологічного панування даних й накопичення протиріч щодо регулювання прав, пов'язаних з їхнім використанням у пандемічну й постпандемічну добу. Тому важливим видається оновлення Закону на основі всебічного урахування норм Регламенту, Угоди про Асоціацію між Україною та ЄС, зокрема пропонується така структуризація напрямів, за якими вбачається доцільність гармонізації законодавства (табл. 2).

Висновки. До магістральних напрямів удосконалення регулювання у сфері захисту персональних даних в Україні, зокрема стосовно зменшення інституційних вразливостей та реалізації потенціалу євроінтеграційних прагнень, пропонується зосередити фахову дискусію у ключових сферах. Так, доцільні консенсусні напрацювання таких змін до законодавства щодо захисту персональних даних:

- розроблення проєкту змін до ст. 4 188-39 КУАП. Передбачити відповідальність за деякі порушення положень Закону, зокрема урахування можливості розширити межі санкцій та залишити це питання на розсуд органу, що виносить рішення про притягнення до відповідальності;
- передбачити створення окремого органу, який наглядав би за дотриманням законодавства щодо захисту персональних даних на кшталт європейського регулятора;
- розглянути доцільність комплексного вирішення проблем регулювання захисту персональних даних в контексті перспективного напряму Національної економічної стратегії на період до 2030 р. «Цифрова економіка» за стратегічною ціллю «Створення нових можливостей для реалізації людського капіталу, розвитку інноваційних, креативних та «цифрових» індустрій і бізнесу», що передбачає проведення затвердження та імплементації цифрових прав, а саме забезпечення гармонізації цифрових прав з найкращими практиками ЄС [23];
- сприяння інноваційно-інституційним перетворенням, пов'язаним із інклюзивним розвитком цифрової інфраструктури, зокрема інтенсифікації секторальної взаємодії із глобальними ініціативами та громадськими рухами щодо ствердження цифрової довіри та прав, пов'язаних із використанням даних на кшталт *Open Digital Trust Initiative* [24];
- випереджальне формування технологічної та організаційної спроможності, зокрема шляхом долучення до спільної дослідницької діяльності у розробленні прикладних проєктів на кшталт *Business Process Re-engineering and functional toolkit for GDPR compliance (https://www.bpr4gdpr.eu/), Data Governance for Supporting GDPR (https://www.defendproject.eu/), GDPR Compliance Cloud Platform for Micro Enterprises (https://smoothplatform.eu/), Methods and tools for GDPR compliance through Privacy and Data Protection Engineering (https://www.pdp4e-project.eu/), PlAtform for PrivAcY preserving data Analytics (https://www.papaya-project.eu/), Protection and control of Secured Information by means of a privacy enhanced Dashboard (https://www.poseidon-h2020.eu/)* [25];

Таблиця 2. **Систематизація пріоритетних напрямів гармонізації європейського та національного регулювання сфери захисту персональних даних**

№ з/п	Пріоритетний напрям удосконалення національного законодавства	Характеристика змісту пріоритетного напряму
1	Уточнення стосовно матеріальної дії Закону	З метою обмеження правового регулювання та уникнення надмірного правового навантаження на фізичних осіб, а також в окремих випадках на органи державної влади, якщо застосуванню підлягають особливі процедури опрацювання персональних даних у межах діяльності таких органів. Тому у новій редакції Закону потрібно передбачити, що його дія не поширюватиметься, зокрема, на оброблення персональних даних органами державної влади, що здійснюється в ході розвідувальної діяльності, спеціальної розвідки, контррозвідувальної діяльності
2	Забезпечення осучаснення категоріально-термінологічного апарату нормативно-правового акта	Перелік категорій, визначення яких повинно бути імплементовано у національну рамку, охоплює, зокрема, «біометричні дані», «витік персональних даних», «контролер персональних даних», «генетичні дані», «дані про стан здоров'я», «психометричні дані», «широкомасштабне оброблення персональних даних», «профілювання», «прямий маркетинг», «псевдонімізація»
3	Упровадження принципів оброблення персональних даних	З метою встановлення фундаментальних орієнтирів для оброблення персональних даних відповідно до міжнародних стандартів. Такими принципами мають бути: законність, добросовісність та прозорість; обмеження мети; мінімізація персональних даних; точність персональних даних; обмеження зберігання; цілісність і конфіденційність; підзвітність. Необхідно розкрити і деталізувати їхній зміст, а також покласти тягар доведення відповідності їм процедур оброблення даних на контролера, що забезпечить додаткову мотивацію для осіб, котрі обробляють дані, дотримуватися вимог законодавства
4	Урегулювання процедур, пов'язаних з наданням згоди на оброблення	Необхідно прив'язати надання згоди суб'єктом даних на оброблення його персональних даних до однієї або кількох точно визначених цілей обробки, що поможе уникнути ситуацій, коли персональні дані використовуються для цілей, які не відповідають волі суб'єкта персональних даних, що надав згоду. Потрібно визначити способи надання згоди суб'єкта даних на оброблення його персональних даних згідно зі стандартами, встановленими Регламентом. Необхідно встановити випадки, які не становлять згоду на обробку персональних даних, зокрема дії суб'єкта персональних даних, які не передбачають волевиявлення, автоматичне заповнення інтерфейсом форми вебсайту або мобільного додатку та власне бездіяльність самого суб'єкта. Необхідно встановити підстави, коли згода не може вважатися вільною. Для забезпечення розуміння суб'єктом, яким чином та ким будуть оброблятися його персональні дані, у новій редакції Закону необхідно передбачити, що такий суб'єкт ще перед опрацюванням даних повинен отримати від контролера додаткову релевантну інформацію (підстава, мета, вид оброблення персональних даних; персональні дані, що підлягають обробленню; контактні дані контролера, його місце розташування та засоби зв'язку з ними; права суб'єкта даних, передбачені законодавством у сфері захисту персональних даних, та способи їх реалізації; будь-яка інша інформація, необхідна для забезпечення чесної та прозорої обробки персональних даних). Для забезпечення гарантій прав дітей у сфері оброблення персональних даних нова редакція Закону має особливості надання ними згоди шляхом встановлення правила, що тоді, коли суб'єктом даних є малолітня особа, згода має бути надана її законним представником

Продовження табл. 2

№ з/п	Пріоритетний напрям удосконалення національного законодавства	Характеристика змісту пріоритетного напряму
5	Усебічне урахування досвіду та стандартів щодо оброблення чутливих персональних даних	По-перше, необхідно розширити перелік чутливих персональних даних, обробка яких забороняється, включивши також дані, що стосуються сексуальної орієнтації, та психометричні дані. По-друге, потрібно розширити перелік винятків, коли обробка чутливих персональних даних допускається, включивши, зокрема, опрацювання даних, які суб'єкт персональних даних явно оприлюднив, або для цілей архівування в суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей, що здійснюється на підставі Закону
6	Урегулювання питань опрацювання персональних даних для іншої мети, ніж та, з якою вони збирались	По-перше, потрібно увести категорію сумісності мети, тобто дозволити оброблення персональних даних для нової мети, якщо нова є сумісною з первинною. Під час визначення сумісності необхідно враховувати передбачені новою редакцією Закону критерії, як-то, наявність зв'язку між первинною метою та новою метою, обставини, за яких персональні дані було зібрано, можливі наслідки обробки даних з новою метою для суб'єкта персональних даних тощо. По-друге, потрібно дозволити оброблення персональних даних для нової мети, якщо суб'єктом даних надана згода на оброблення даних з новою метою або ж таке оброблення необхідне для виконання юридичного обов'язку, передбаченого законом, що містить належні гарантії для захисту прав і свобод суб'єкта персональних даних
7	Регламентація реалізації прав суб'єктів персональних даних, зокрема права на інформацію, права на доступ, права на виправлення персональних даних, права на забуття, права на мобільність персональних даних, права на обмеження оброблення персональних даних, права на захист від автоматизованого ухвалення рішення, права суб'єкта даних на захист своїх прав та відшкодування шкоди	Щодо права на інформацію, необхідно передбачити детальний перелік інформації, який має бути повідомлений суб'єкту персональних даних під час отримання персональних даних, а також випадки обмеження цього права, зокрема, якщо таке обмеження передбачене законом, переслідує легітимну мету та є пропорційним. Щодо права на виправлення, нова редакція Закону має надати можливість суб'єкту висувати вимогу до контролера щодо виправлення контролером неточних персональних даних без надмірної затримки в строк не більше тридцяти днів, а також можливість суб'єкта даних доповнити свої персональні дані шляхом надання додаткових даних контролеру. Щодо права на забуття, суб'єкт даних має мати здатність вимагати знищення контролером його персональних даних без надмірної затримки у разі: 1) якщо відсутня необхідність подальшого оброблення персональних даних, для цілей, для яких вони збирались або оброблялись; 2) якщо відкликана згода; 3) якщо суб'єкт персональних даних заперечує проти оброблення; 4) якщо опрацювання здійснювалась незаконно; 5) якщо персональні дані зібрано для пропозиції суб'єкту персональних даних послуг інформаційного суспільства. Суб'єкту персональних даних необхідно надати право заперечення в будь-який час проти оброблення його персональних даних та встановити кореспондуючий обов'язок контролера припинити у такому разі подальшу обробку. Нова редакція Закону повинна також регламентувати право суб'єкта вимагати від контролера надання копії будь-яких персональних даних такого суб'єкта, зібраних контролером під час автоматизованої оброблення у структурованому та машинозчитуваному форматі. Щодо права на обмеження, суб'єкт персональних даних повинен мати можливість обмежити оброблення у випадку настання визначених новою редакцією Закону підстав, зокрема, якщо суб'єкт персональних даних оскаржив точність персональних даних або якщо оброблення персональних даних є незаконним і суб'єкт персональних даних заперечує проти видалення персональних даних і натомість вимагає обмежити їхнє використання тощо. Новою редакцією Закону потрібно також надати право суб'єкту персональних даних звернутись із скаргою на порушення його прав до органу контролю або до суду та вимагати відшкодування матеріальної та/або моральної шкоди,

Продовження табл. 2

№ з/п	Пріоритетний напрям удосконалення національного законодавства	Характеристика змісту пріоритетного напряму
		завданої внаслідок порушення його прав. Для цього потрібно визначити на загальному рівні у новій редакції Закону порядок розгляду вимог суб'єкта персональних даних у разі звернення із заявою до контролера, зокрема, визначити зміст заяви, форму її подачу (письмова та електронна) та строк обрання рішення контролером (1 місяць)
8	Деталізація рівнів визначення обов'язків і відповідальності контролера та оператора персональних даних	Покласти на контролера загальний обов'язок вживати належних технічних та організаційних заходів для забезпечення оброблення даних відповідно до вимог цього закону та спроможності довести. Встановити стандарт оброблення даних за призначенням і за замовчуванням, відповідно до якого захист має бути частиною розроблення бізнес-процесів, продуктів і послуг. Налаштування конфіденційності повинні бути встановлені на високому рівні за замовчуванням, і контролер має здійснити технічні та процедурні заходи, щоб забезпечити дотримання регламенту протягом усього життєвого циклу опрацювання даних. Регламентувати розподіл обов'язків у разі оброблення даних спільними контролерами, наприклад, на підставі договору про розподіл обов'язків щодо дотримання вимог обробки персональних даних. Визначити зміст договору, яким оператор уповноважується контролером на оброблення даних. Такий договір повинен охоплювати умови, якими встановлюються обов'язки оператора, зокрема, здійснювати будь-яку діяльність винятково за наявності письмового доручення контролера, допускати до оброблення персональних даних лише тих осіб, на яких поширюється зобов'язання щодо збереження конфіденційності інформації, надавати допомогу та сприяння у дотриманні контролером обов'язку відповідати на запити суб'єктів даних щодо реалізації їхніх прав, за вимогою контролера видалити або повернути всі персональні дані контролеру після закінчення строку надання послуг з оброблення даних тощо. Покласти обов'язок на контролера здійснювати реєстрацію операцій з оброблення персональних даних, за яку він несе відповідальність, і визначити перелік інформації, яку має містити такий запис, а також передбачити обов'язок надання таких записів органу контролю у відповідь на запит. З метою уникнення надмірного обтяження малого бізнесу така вимога не має поширюватися на суб'єктів оброблення з чисельністю працівників менше ніж 10 осіб. Встановити вимоги щодо безпечності оброблення персональних даних шляхом вживанням контролером або оператором належних заходів технічного та організаційного характеру, які можуть охоплювати псевдонімізацію та шифрування персональних даних, безперервне забезпечення конфіденційності, цілісності, доступності персональних даних і стійкості систем. і сервісів оброблення, забезпечення своєчасного відновлення доступу до персональних даних у разі виникнення аварійної ситуації або інциденту, регулярне тестування, оцінювання та вимірювання ефективності заходів тощо. Визначити обов'язки співпраці контролера та оператора з органом контролю шляхом забезпечення доступу до приміщень, матеріалів і документів, надання інформації та пояснення стосовно фактичної і правової підстави своїх дій і рішень, пов'язаних з обробленням персональних даних, а також детально регламентувати здійснення контролером повідомлення органу контролю про витік персональних даних, встановивши строки (до 72 годин) та зміст такого повідомлення. Покласти обов'язок на контролера здійснювати оцінку впливу оброблення персональних даних на захист персональних даних до початку такої обробленя, якщо використання нових технологій або характер, обсяг, контекст та цілі обробки ймовірно призведуть до настання ризику високого рівня для прав та свобод фізичної особи, регламентувати випадки обов'язкового здійснення такої оцінки та визначити складові змісту висновку, що складаються за наслідком такої оцінки, а також покласти на контролера обов'язок провести попередню консультацію з органом контролю до початку обробки персональних даних,

Закінчення табл. 2

№ з/п	Пріоритетний напрям удосконалення національного законодавства	Характеристика змісту пріоритетного напряму
		якщо оцінка впливу свідчить, що оброблення персональних даних ймовірно може призвести до настання високого ступеня ризиків. Визначити випадки, коли контролер та оператор зобов'язані призначити відповідальну особу з питань захисту персональних даних, у разі, якщо оброблення персональних даних здійснюється суб'єктом владних повноважень або основна діяльність контролера або оператора полягає в обробленні персональних даних, що вимагає регулярного та систематичного широкомасштабного моніторингу дій або бездіяльності суб'єктів персональних даних тощо. Регламентувати обов'язки відповідальної особи з питань захисту персональних даних, встановити кваліфікаційні умови її призначення та гарантії незалежності
9	Урегулювання аспектів питання транскордонної передачі персональних даних	Підставами для передачі персональних даних іншим державам та/або міжнародним організаціям можуть бути такі: інша держава або міжнародна організація забезпечує належний рівень захисту персональних даних; контролер та/або оператор надав належні гарантії захисту персональних даних; затверджені обов'язкові корпоративні правила; інші підстави (наприклад, надання явної згоди суб'єкта даних). Для цього також необхідно буде визначити критерії встановлення відповідності рівня захисту іншої держави та/або організації, визначити належні гарантії захисту персональних даних, які дозволяють контролеру або оператору передавати дані без дозволу органу контролю, а також встановити зміст обов'язкових корпоративних правил, які дозволяють передачу персональних даних на територію іншої держави в межах однієї групи підприємств
10	Урахування положень Регламенту щодо настання відповідальності за порушення у сфері персональних даних	Передбачити, що рішення про притягнення до відповідальності за правопорушення у сфері захисту персональних даних ухвалюється органом контролю і до такої відповідальності можуть бути притягнені контролери або оператори персональних даних. Запровадити правило, згідно з яким кожен контролер або оператор несе відповідальність за усю шкоду, заподіяну з їхньої вини. Надати право суб'єктам персональних даних на відшкодування матеріальної та моральної шкоди, завданої внаслідок порушення його прав, у порядку, передбаченому цивільним законодавством незалежно від притягнення винних осіб до відповідальності. Здійснити диференціацію правопорушень, а також санкцій, зробивши їх суворішими порівняно з поточними санкціями, встановленими Кодексом України з адміністративних правопорушень

• розробити редакцію докорінного оновлення Закону на основі всебічного урахування норм Регламенту, Угоди про Асоціацію між Україною та ЄС, із структуризацією напрямів, за якими вбачається доцільність гармонізації законодавства.

Водночас деякі концепції та положення Регламенту не повинні бути перенесені до нової редакції Закону. Так, українські реалії не потребують функціонування наглядових установ, які створюються Регламентом з урахуванням особливостей системи ЄС, як-то Європейської ради із захисту даних. Іншим прикладом положень Регламенту, які не повинні бути враховані повною мірою у новій редакції Закону, є розміри штрафних санкцій за порушення у сфері захисту персональних даних, адже система відповідальності за певні порушення повинна відповідати доктрині правової відповідальності за українським правом. Насамкінець, нова редакція Закону не повинна містити положень Регламенту, які є характерними суто для системи ЄС. Прикладом таких норм є ст. ст. 92 і 93 Регламенту, які стосуються здійснення контролю країн — членів ЄС над Європейською Комісією під час реалізації нею імплементаційних повноважень. Для цілей забезпечення ефективного

контролю за дотриманням законодавства у сфері персональних даних необхідно також створити ефективний наглядовий орган, який буде забезпечений достатніми гарантіями незалежності і самостійності і якому на належному рівні буде забезпечена інституційна спроможність для реалізації регуляторних і контрольних функцій. Законом відповідні повноваження покладені на Уповноваженого Верховної Ради з питань прав людини, який наразі не є спроможним забезпечувати на належному рівні реалізацію державною політики у цій сфері.

Отже, існує потреба утворення нового органу державного контролю у сфері персональних даних, який буде інституційно спроможним виконувати завдання та реалізовувати відповідні повноваження для забезпечення належного захисту персональних даних в Україні. У новій редакції Закону з урахуванням стандартів, передбачених Регламентом, мають бути визначені модель функціонування такого органу та його правовий статус із наданням особливої уваги питанням забезпечення його незалежності і самостійності. Така мета може бути досягнута шляхом встановлення особливих вимог до членів органу контролю, упровадження прозорої процедури їхнього призначення, забезпечення фінансової незалежності органу та надання йому достатніх повноважень.

Забезпечення функціонування органу державного контролю у сфері персональних даних є важливим, особливо з огляду на необхідність отримання Україною рішення Європейської Комісії про адекватність захисту персональних даних, що дозволить здійснювати безперешкодно передачу персональних даних з ЄС до України. Існування та ефективне функціонування незалежного органу контролю, який забезпечує виконання правил стосовно захисту персональних даних, є одним із факторів, що враховуються Європейською Комісією під час ухвалення рішення про адекватність. Іншими факторами є законодавство, судова практика, ефективні адміністративні та судові інструменти захисту прав суб'єктів даних, а також міжнародні зобов'язання України щодо захисту персональних даних. Рішення Європейської Комісії про адекватність захисту персональних даних в Україні підлягатиме перегляду кожні чотири роки. У разі оновлення українського правового регулювання відповідно до вимог Регламенту, а також якісного забезпечення функціонування наглядового органу, стандарти захисту персональних даних в Україні будуть істотно наближені до європейських.

СПИСОК ЛІТЕРАТУРИ

1. First report on the implementation of the Data Protection Directive (95/46/EC). *Official website of the European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52003DC0265 (дата звернення: 06.11.2021).
2. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official website of the European Union.* URL: https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (дата звернення: 06.11.2021).
3. EU Member States notifications to the European Commission under the GDPR. *Official website of the European Union.* URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en (дата звернення: 06.11.2021).
4. Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law.* 2019. Vol. 28. No.1. P. 65—98. https://doi.org/10.1080/13600834.2019.1573501
5. Satariano A. Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates. *The New York Times.* 2020. URL: https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html (дата звернення: 06.11.2021).
6. Three years under the EU GDPR an implementation progress report. *Access Now.* URL: https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf (дата звернення: 06.11.2021).
7. Kuner C. Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. *University of Cambridge Faculty of Law Research Paper No. 20/2021.* April 16, 2021. http://dx.doi.org/10.2139/ssrn.3827850
8. Daigle B., Khan M. EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities. *Journal of International Commerce and Economics.* June, 2020. URL: https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf (дата звернення: 06.11.2021).

9. Пояснювальна записка до проєкту Закону України «Про захист персональних даних» (реєстр. № 5628 від 07.06.2021) *Офіційний портал Верховної Ради України*. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=32124&pf35401=119742 (дата звернення: 06.11.2021).
10. Про затвердження документів у сфері захисту персональних даних: наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. *Офіційний портал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text (дата звернення: 06.11.2021).
11. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. *Офіційний портал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 06.11.2021).
12. Венгер В., Заярний О. Правовий аналіз основних моделей інституалізації державного контролю у сфері персональних даних та доступу до публічної інформації. *Council of Europe*. 2020. URL: https://rm.coe.int/legal-analysis-data-ua/16809ee077 (дата звернення: 06.11.2021).
13. Козлов С. Скандал! Цифра? Дія... *Юридична газета*. 2020. 2 черв. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/skandal-cifra-diya.html (дата звернення: 06.11.2021).
14. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2019 рік. *Уповноважений Верховної Ради України з прав людини*. URL: https://ombudsman.gov.ua/files/Dopovidi/zvit%20za%202019.pdf (дата звернення: 06.11.2021).
15. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2020 рік. *Уповноважений Верховної Ради України з прав людини*. URL: https://ombudsman.gov.ua/files/2021/zvit_2020_rik_.pdf (дата звернення: 06.11.2021).
16. Матола В. «Баги» державних реєстрів, або як захистити персональні дані. *LB.ua*. URL: https://lb.ua/pravo/2020/05/19/457892_bagi_derzhavnih_reiestriv_abo_yak.html (дата звернення: 06.11.2021).
17. Постанова Верховного Суду від 30.01.2019 у справі № 308/5318/15-ц. *Єдиний державний реєстр судових рішень*. URL: http://reyestr.court.gov.ua/Review/79744914 (дата звернення: 06.11.2021).
18. Рішення Львівського окружного адміністративного суду від 21.01.2019 у справі № 813/2804/18. *Єдиний державний реєстр судових рішень*. URL: http://reyestr.court.gov.ua/Review/79279901?fbclid=IwAR3ghlUuzjsm88qkmjPlhloHwLa3-itR1Dd-2yzTalxiZcVZJze9qgASvXM (дата звернення: 06.11.2021).
19. Ухвала Окружного адміністративного суду м. Києва від 18.10.2019 у справі № 640/19197/19. *Єдиний державний реєстр судових рішень*. URL: http://reyestr.court.gov.ua/Review/85054313 (дата звернення: 06.11.2021).
20. Вирок Заводського районного суду м. Дніпродзержинська від 25.07.2019 у справі № 200/6814/19. *Єдиний державний реєстр судових рішень*. URL: http://reyestr.court.gov.ua/Review/83313961 (дата звернення: 06.11.2021).
21. Постанова Подільського районного суду м. Києва від 07.022020 у справі № 758/14158/19. *Єдиний державний реєстр судових рішень*. URL: http://reyestr.court.gov.ua/Review/87632133 (дата звернення: 06.11.2021).
22. «Суріков проти України»: Зберігання роботодавцем медичних даних співробітників можливе лише за умови їх строгої конфіденційності, постійного оновлення та використання виключно з метою їх збору (ст. 6 та 8 Конвенції, заява № 42788/06 від 26.01.2017). *Протокол. Юридичний інтернет ресурс*. URL: https://protocol.ua/ua/surikov_proti_ukraini (дата звернення: 06.11.2021).
23. Національна економічна стратегія на період до 2030 року, затверджена постановою Кабінету Міністрів України від 03.03.2021 № 179. *Офіційний портал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/file/text/88/f503442n31.doc (дата звернення: 06.11.2021).
24. Open Digital Trust Initiative. *Institute of International Finance*. URL: https://www.iif.com/Innovation/Open-Digital-Trust-Initiative (дата звернення: 06.11.2021).
25. de Carvalho R.M., Del Prete C., Martin Y.S. et al. Protecting Citizens' Personal Data and Privacy: Joint Effort from GDPR EU Cluster Research Projects. SN *Computer Science*. 2020. No. 1. Art. No. 217. https://doi.org/10.1007/s42979-020-00218-8

Надійшла 12.12.2021

REFERENCES

1. First report on the implementation of the Data Protection Directive (95/46/EC). *Official website of the European Union*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52003DC0265
2. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official website of the European Union*. URL: https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf
3. EU Member States notifications to the European Commission under the GDPR. *Official website of the European Union*. URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en
4. Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*. 2019. Vol. 28. No. 1. P. 65-98. https://doi.org/10.1080/13600834.2019.1573501
5. Satariano A. Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates. *The New York Times*. 2020. URL: https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html

6. Three years under the EU GDPR an implementation progress report. *Access Now.* URL: https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf
7. Kuner, C. Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. *University of Cambridge Faculty of Law Research Paper No. 20/2021.* April 16, 2021. http://dx.doi.org/10.2139/ssrn.3827850
8. Daigle, B., Khan, M. EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities. *Journal of International Commerce and Economics.* June, 2020. URL: https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf
9. Poiasniuvalna zapyska do proiektu Zakonu Ukrainy "Pro zakhyst personalnykh danykh" (reiestr. No. 5628 vid 07.06.2021) *Ofitsiinyi portal Verkhovnoi Rady Ukrainy.* URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=32124&pf35401=119742 [in Ukrainian].
10. Pro zatverdzhennia dokumentiv u sferi zakhystu personalnykh danykh: nakaz Upovnovazhenoho Verkhovnoi Rady Ukrainy z prav liudyny vid 08.01.2014 No. 1/02-14. *Ofitsiinyi portal Verkhovnoi Rady Ukrainy.* URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text [in Ukrainian].
11. Uhoda pro asotsiatsiiu mizh Ukrainoiu, z odniiei storony, ta Yevropeiskym Soiuzom, Yevropeiskym spivtovarystvom z atomnoi enerhii i yikhnimy derzhavamy-chlenamy, z inshoi storony. *Ofitsiinyi portal Verkhovnoi Rady Ukrainy.* URL: https://zakon.rada.gov.ua/laws/show/984_011#Text [in Ukrainian].
12. Venher V., Zaiarnyi O. Pravovyi analiz osnovnykh modelei instytualizatsii derzhavnoho kontroliu u sferi personalnykh danykh ta dostupu do publichnoi informatsii. *Council of Europe.* 2020. URL: https://rm.coe.int/legal-analysis-data-ua/16809ee077 [in Ukrainian].
13. Kozlov S. Skandal! Tsyfra? Diia... *Yurydychna hazeta.* 2020. 2 chervnia. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/skandal-cifra-diya.html [in Ukrainian].
14. Shchorichna dopovid Upovnovazhenoho Verkhovnoi Rady Ukrainy z prav liudyny pro stan doderzhannia ta zakhystu prav i svobod liudyny i hromadianyna v Ukraini 2019 rik. *Upovnovazhenyi Verkhovnoi Rady Ukrainy z prav liudyny.* URL: https://ombudsman.gov.ua/files/Dopovidi/zvit%20za%202019.pdf [in Ukrainian].
15. Shchorichna dopovid Upovnovazhenoho Verkhovnoi Rady Ukrainy z prav liudyny pro stan doderzhannia ta zakhystu prav i svobod liudyny i hromadianyna v Ukraini 2020 rik. *Upovnovazhenyi Verkhovnoi Rady Ukrainy z prav liudyny.* URL: https://ombudsman.gov.ua/files/2021/zvit_2020_rik_.pdf [in Ukrainian].
16. Matola V. "Bahy" derzhavnykh reiestriv, abo yak zakhystyty personalni dani. *LB.ua.* URL: https://lb.ua/pravo/2020/05/19/457892_bagi_derzhavnih_reiestriv_abo_yak.html [in Ukrainian].
17. Postanova Verkhovnoho Sudu vid 30.01.2019 u spravi No. 308/5318/15-ts. Yedynyi derzhavnyi reiestr sudovykh rishen. URL: http://reyestr.court.gov.ua/Review/79744914 [in Ukrainian].
18. Rishennia Lvivskoho okruzhnoho administratyvnoho sudu vid 21.01.2019 u spravi No. 813/2804/18. *Yedynyi derzhavnyi reiestr sudovykh rishen.* URL: http://reyestr.court.gov.ua/Review/79279901?fbclid=IwAR3ghlUuzjsm88qkmjPlhloHwLa3-itR1Dd-2yzTalxiZcVZJze9qgASvXM [in Ukrainian].
19. Ukhvala Okruzhnoho administratyvnoho sudu m. Kyieva vid 18.10.2019 u spravi No. 640/19197/19. *Yedynyi derzhavnyi reiestr sudovykh rishen.* URL: http://reyestr.court.gov.ua/Review/85054313 [in Ukrainian].
20. Vyrok Zavodskoho raionnoho sudu m. Dniprodzerzhynska vid 25.07.2019 u spravi No. 200/6814/19. *Yedynyi derzhavnyi reiestr sudovykh rishen.* URL: http://reyestr.court.gov.ua/Review/83313961 [in Ukrainian].
21. Postanova Podilskoho raionnoho sudu m. Kyieva vid 07.022020 u spravi No. 758/14158/19. *Yedynyi derzhavnyi reiestr sudovykh rishen.* URL: http://reyestr.court.gov.ua/Review/87632133 [in Ukrainian].
22. "Surikov proty Ukrainy": Zberihannia robotodavtsem medychnykh danykh spivrobitnykiv mozhlyve lyshe za umovy yikh strohoi konfidentsiinosti, postiinoho onovlennia ta vykorystannia vykliuchno z metoiu yikh zboru (st. 6 ta st.8 Konventsii, zaiava No. 42788/06 vid 26.01.2017). *Protokol. Yurydychnyi internet resurs.* URL: https://protocol.ua/ua/surikov_proti_ukraini [in Ukrainian].
23. Natsionalna ekonomichna stratehiia na period do 2030 roku, zatverdzhena postanovoiu Kabinetu Ministriv Ukrainy vid 03.03.2021 No. 179. *Ofitsiinyi portal Verkhovnoi Rady Ukrainy.* URL: https://zakon.rada.gov.ua/laws/file/text/88/f503442n31.doc [in Ukrainian].
24. Open Digital Trust Initiative. *Institute of International Finance.* URL: https://www.iif.com/Innovation/Open-Digital-Trust-Initiative
25. de Carvalho, R.M., Del Prete, C., Martin, Y.S. et al. Protecting Citizens' Personal Data and Privacy: Joint Effort from GDPR EU Cluster Research Projects. *SN Computer Science.* 2020. No. 1. Art. No. 217. https://doi.org/10.1007/s42979-020-00218-8

Received 12.12.2021

Ya.V. Kotlyarevskyy
Ministry of Finance of Ukraine, Kyiv, Ukraine
orcid.org/0000-0003-3542-6952
M.V. Siryk
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
orcid.org/0000-0002-0588-2183
M.O. Diachenko
Partnership Network "Education for Sustainable Development", SGP GEF-UNDP expert, Kyiv, Ukraine
orcid.org/0000-0002-7518-3038

PROSPECTIVE DIRECTIONS FOR IMPROVING THE REGULATION OF PERSONAL DATA PROTECTION IN UKRAINE

The process of legislative settlement of issues related to the protection of personal data began in the European Union (EU) with the entry into force of Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals regarding the processing of personal data and on the free movement of such data (Directive). After adoption the Charter of Fundamental Rights of the European Union (2000), which Article 8 defined the protection of personal data as a human right, establishment of the sufficient principles in the Lisbon Treaty (2009), there were amended two key EU acts: the Treaty on EU and the Treaty establishing the European Community. As a result, everyone in the EU was guaranteed the right to protect their personal data. In 2016 the EU adopted Regulation 2016/679/EC of the European Parliament and of the Council on the protection of natural persons regarding the processing of personal data and on the free movement of such data (Regulation), which radically updated the methods of collecting and processing personal data, and not only in the EU. As a result, to comply with its requirements, both EU-based companies and those operating in the EU or working with consumers from the EU market were forced to update their privacy/personal data policies.
In turn, in Ukraine, significant progress in the development of legal regulation of personal data protection occurred later. As of 2010, public relations regarding collection, storage, use and dissemination of information about a person were regulated by more than two dozen uncoordinated laws and secondary legislation. To specify and define the mechanisms for implementing the provisions of Article 32, Constitution of Ukraine, which proclaimed the right of a person to non–interference in its personal life and established a ban on the collection, storage, use and dissemination of confidential information about a person without its consent, the Verkhovna Rada of Ukraine in 2010 adopted the law of Ukraine "On Personal Data Protection". Having played a vital role in the legislative codification of the rules for processing personal data, the law, like the Directive, failed to respond to technological changes and the processes caused by this in society, despite numerous amendments made by MPs.
Since the Association Agreement between EU and Ukraine came into power, there is noticeable arising necessity to harmonize the Ukrainian legislative framework with EU, as though contexts of adoption of the Regulation and the Law are different, so are the ways of resolving personal protection issues in Ukraine and the EU. Therefore, it is necessary to establish the new legislative amendments, the degree of compliance of personal data protection standards in Ukraine with the relevant standards in the EU. In this paper, as an outcome of estimations of relevant international research, further analytical and comparative analyses, there are some proposals to future institutional features of such modernization, affecting such issues as: clarification regarding material effects in order to limit legal regulation and avoid excessive legal burden on individuals, as well as in some cases on state authorities; providing new definitions of concepts that are not yet available in domestic regulation; establishment of fundamental guidelines for the processing of personal data in accordance with international standards; fostering more sustainable standards for the processing of sensitive personal data; in-depth structuring the issue of processing personal data for a different purpose than the one for which they were collected; regulating the implementation of the rights of personal data subjects, in particular, the right to information, the right to access, the right to correct personal data, the right to be forgotten, the right to personal data mobility, the right to restrict the processing of personal data, the right to protection from automated decision-making, the right of the data subject to protection of their rights and compensation for damage; clarifications regarding the definitions of the duties and responsibilities of the personal data controllers and operator; sustainable regulations concerning the issue of cross-border transfer of personal data.

Keywords: personal data, regulation, institutional support, international experience.