УДК 342.5:341.1
DOI https://doi.org/10.24144/2307-3322.2024.82.2.39

НАЦІОНАЛЬНІ ОРГАНИ ЗАХИСТУ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ: РОЛЬ І ПРАКТИКА В СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ

Пристай Р.А.,
аспірант кафедри адміністративного та фінансового права
ЛНУ ім. Івана Франка
ORCID: https://orcid.org/0000-0002-8980-1650
e-mail: rostyslaw.law@gmail.com

Пристай Р.А. Національні органи захисту даних в Європейському Союзі: роль і практика в сфері захисту персональних даних в соціальних мережах.

В статті досліджено особливості законодавчого регулювання та практичної діяльності національних органів з захисту персональних даних в Європейському Союзі (Data Protection Authorities (DPA)). Проаналізовано положення Загального регламенту про захист даних (Genereal Data Protection Regulation), Директиви Європейського Парламенту та Ради від 14 грудня 2022 року про заходи щодо високого загального рівня кібербезпеки в Союзі, а також інші акти, прийняті в рамках ЄС в сфері захисту персональних даних, інформаційної та кібербезпеки. Досліджено нормативні передумови створення та роль національних органів з захисту персональних даних в забезпеченні приватності та захищеності персональних даних користувачів соціальних мереж, а саме: нормативні положення, які забезпечують їх організацію, компетенцію, можливості здійснення транскордонної кооперації та співробітництва (joint investigation) а також вплив на діяльність сервісів соціальних мереж в конкретних державах. Проаналізовано практику національних органів з захисту персональних даних держав-членів в ЄС в контексті вжиття дій, пов'язаних із захистом персональних даних в соціальних мережах – розслідування, накладення штрафів, звернення до національних судових установ, розробки вимог до оцінки впливу на захист даних, а також створення кодексів поведінки та сертифікації. На основі отриманих результатів запропоновано висновки щодо доцільності створення зазначених органів в Україні, рекомендації щодо механізму їх організації, доцільності надання імперативного характеру рішенням вказаних органів, а також необхідності створення сприятливих умов для співробітництва з іншими національними та міжнародними публічними органами з захисту персональних даних. З вказаною метою, здійснено додатковий аналіз можливостей впливу національних органів з захисту даних на функціонування сервісів соціальних мереж поза юрисдикцією держав-членів ЄС.

Ключові слова: захист персональних даних, національні органи з захисту даних, соціальні мережі, право Європейського Союзу.

Prystai R. National Data Protection Authorities in the EU: role and practice in the field of personal data protection in social networks.

Internal violations of the legislation of personal data protection by online social network services is a problem faced by all states, regardless of the presence or absence of national bodies for monitoring compliance with the legislation on the protection of personal data. However, the key differences that distinguish countries that have relevant authorities from those that do not have any or are entrusted with an authority that is unable to adequately perform the function of data protection are: a lower level of violations of privacy and personal data in social networks; the presence of a real possibility of the state tp protect privacy and personal data in the form of an authorized body, as well as the citizens themselves, to effectively protect their personal data; the ability of the state to flexibly determine the policy and conditions under which this or that social network service will carry out its activities on its territory.

Thus, the article examines the peculiarities of legislative regulation and practical activities of national bodies for the protection of personal data in the European Union (Data Protection Authorities (DPA)). The

regulatory basis and role in ensuring the privacy and security of personal data of users of social networks have been studied, namely: the grounds for implementation, regulatory provisions that ensure their organization, competence, opportunities for cross-border cooperation and cooperation (joint investigation), as well as the impact on the activity of social services networks in specific countries. The practice of national bodies for the protection of personal data of member states in the EU was analyzed in the context of taking actions related to the protection of personal data in social networks - investigations, imposition of fines, appeals to national judicial institutions, development of requirements for Data Protection Impact Assessment (DPIA) as well as the creation of codes of conduct and certification. On the basis of the obtained results, conclusions regarding the need to introduce separate national data protection authorities in Ukraine are proposed, as well the possibility of DPA influence on the functioning of social network services outside the jurisdiction of the EU member state is outlined.

Key words*:* Personal Data protection, Data Protection Authorities, social networks, EU legislation.

Постановка проблеми. Після набрання чинності а також вступу в дію в травні 2018-го року Регламенту Європейського парламенту і Ради ЄС (2016/679) [1] про захист фізичних осіб у зв'язку з опрацюваням персональних даних і про вільний рух таких даних (Загального регламенту про захист даних, або ж GDPR), загальнообов'язковою стала вимога про створення кожною державою-членом ЄС одного або ж кількох незалежних публічних органів, які повинні відповідати за моніторинг дотримання Регламенту (стаття 51 Регламенту). До цього, аналогічне положення містилось в статті 28 Директиви 95/46 ЕС [2], яка передувала GDPR. Так, національні органи з захисту персональних даних в державах-членах ЄС існують ще з 1995 року, в той час як в Україні, наприклад, такий орган був створений лише в 2011-му році під назвою Державна служба України з питань захисту персональних даних [3; 4], і зміг проіснувати лише до 2014-го року, оскільки був ліквідований і відповідні повноваження були покладені на Уповноваженого Верховної Ради України з прав людини [5]. Втім, доцільність прийняття такого рішення є сумнівною, зважаючи на відсутність прикладів ефективності існуючої національної системи захисту даних та багаторічну практику існування аналогічних органів в інших державах – а саме кількість накладених штрафів за порушення Регламенту, ініціювання та затвердження типових договірних положень, кодексів поведінки, створення механізмів сертифікації захисту даних, проведення розслідувань порушення персональних даних у формі аудиту чи проведення перевірки виданих сертифікатів, видачі доган чи призупиненні потоків даних [6].

Стосовно сфери соціальних мереж. Внутрішні порушення законодавства про захист персональних даних (спричинені умисно, або ж внаслідок недбалих дій сервісу з надання послуг соціальних мереж) – такі як неналежний технічний захист (неправильне зберігання інформації, старі версії сервісів і протоколів передачі гіпертексту, відкриті протоколи передачі файлів [7]), незаконна обробка даних, передача або розкриття даних третім особам, нечіткі умови політик конфіденційності, неналежно оформлені договори з користувачем, – є проблемою, з якою стикаються всі держави, незалежно від наявності чи відсутності в них національних органів з контролю за дотримання законодавства про захист персональних даних. Однак, ключовими відмінностями, які відрізняють держави, в яких існують відповідні органи від тих, в яких вони відсутні або ж покладені на орган, який не в змозі належним чином виконувати функцію захисту даних, є: а) менший рівень порушень приватності та персональних даних в соціальних мережах; б) наявність реальної можливості держави в особі уповноваженого органу, а також самих громадян ефективно захищати свої персональні дані; в) можливість держави гнучко визначати політику та умови, на яких той чи інший сервіс соціальних мереж буде здійснювати свою діяльність на її території.

Таким чином, доцільним є дослідження правової природи та ролі національних органів з захисту персональних даних, їх реальних можливостей і повноважень щодо захисту персональних даних особи в соціальних мережах, практики такого захисту, його ефективності а також доцільності створення відповідного адміністративного механізму захисту даних в Україні.

Стан опрацювання. Питання діяльності національних органів захисту персональних даних досліджували Shültz P., Giurgiu A., Larsen A., European Univerity Institute, United States International Trade Commission, Council of Europe, Deloitte, Human Rights Watch та ін. науковці, навчальні заклади, юридичні компанії і міжнародні організації.

Метою статті є дослідження правової природи та ролі національних органів з захисту персональних даних в сфері захисту персональних даних в соціальних мережах.

Основний виклад матеріалу. Органи захисту даних і соціальні мережі в Україні. В Україні станом на липень 2022 року кількість користувачів соціальних мереж становить 76,6% від загальної кількості населення [8]. Відповідні компанії (You Tube, Google, Facebook (Meta), LinkedIn, Telegram, а також окремі мобільні додатки, які хоч і не є соціальними мережами, однак мають доступ до персональних даних особи) збирають значний обсяг конфіденційної інформації користувачів з України. Facebook здійснює збір персональної інформації і поза межами своєї платформи – IP адреса користувача, відвідані ним сайти, вид браузера, який використовується, та багато іншої особистої інформації [9]. Така діяльність соціальних мереж та мобільних додатків на території України створює ризик порушення персональних даних і приватності особи – наприклад, передачу даних третім особам, розкриття інформації про особу, крадіжки персональних даних, незаконного використання персональних даних (таргетована реклама, втручання в приватне життя особи), неможливість видалення своїх даних або ж доступ до них та ін. Так, у випадку порушення приватності особи внаслідок недотримання сервісом вимог законодавства України про захист персональних даних, єдиним органом, до якого можна звернутись в адміністративно-правовому порядку є Уповноважений Верховної Ради України з прав людини, ефективність якого є менш досконалою в порівнянні з існуючою практикою держав-членів ЄС, де для цього створені окремі спеціалізовані органи з захисту персональних даних, що підтверджується офіційно оприлюдненою статистикою та прикладами накладення санкцій на відповідних суб'єктів.

Станом на сьогодні основним нормативним актом, який запроваджує та врегульовує діяльність національних органів із захисту персональних даних (Data Protection Authorites) в державах-членах ЄС є Загальний регламент про захист даних (статті 4(16), Розділ VI (статті з 51 по 59) і декларації (117) – (123)) та Інструкції щодо визначення контролера або головного наглядового органу процесора [10]. Окрім Регламенту, діяльності національних органів з захисту персональних даних стосуються акти м'якого права, наприклад Рекомендації ОБСЄ щодо транскордонного співробітництва у забезпеченні виконання законів про захист приватності (OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy [11]) та положення окремих Регламентів чи Директив Ради ЄС стосовно співробітництва органів з кібербезпеки та наглядових органів (Наприклад, відповідно до статті 2 Директиви (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи щодо високого загального рівня кібербезпеки в Союзі, компетентні органи повинні працювати в тісній співпраці з наглядовими органами відповідно до Регламенту (ЄС) 2016/679 під час розгляду інцидентів, що спричинили порушення персональних даних, без шкоди для компетенції та завдань наглядових органів згідно з цим Регламентом [12]). Інші положення, що стосуються можливості залучення національних органів з захисту персональних даних щодо розслідування відповідних інцидентів які спричинили порушення персональних даних, містяться в національному законодавстві держав-членів ЄС – профільних законах та підзаконних нормативно-правових актах, які передбачають створення та деталізують повноваження відповідних наглядових органів. Сюди належать, наприклад, Закон про захист персональних даних у Німеччині (BDSG – Bundesdatenschutzgesetz, секція 8 – Федеральний уповноважений із захисту даних і свободи інформації [13]), Закон про захист персональних даних у Франції (Loi Informatique et Libertés – Національна комісія з питань інформатики та свободи – CNIL), Закон про захист персональних даних в Італії (Закон No. 675 від 31 грудня 1996 р. та Codice in materia di protezione dei dati personali, які регулюють запровадження органу Гаранта захисту персональних даних), Закон про захист персональних даних в Польщі (Ustawa o Ochronie Danych Osobowych [14], який запроваджує створення Управління та посаду Президента Управління захисту персональних даних) тощо.

Вказані органи створені в межах кожної держави-члена Європейського Союзу. Громадяни можуть звернутись за захистом своїх прав безпосередньо та в онлайн- режимі. Захист персональних даних здійснюється шляхом заповнення відповідних електронних форм та заяв, а структура сайтів дозволяє відслідкувати стан опрацювання відповідних звернень, ознайомитись із законодавством в сфері захисту персональних даних, а також з попередніми рішеннями, звітністю та практикою відповідних органів. Захист персональних даних здійснюється в загальному порядку і в межах органів не функціонують окремі відділи чи департаменти, які б здійснювали захист даних саме в соціальних мережах, – натомість кожна заява розглядається окремо і в загальному порядку відповідності Регламенту в межах компетенції відповідного органу.

Роль та повноваження національних органів з захисту персональних даних в контексті забезпечення приватності в соціальних мережах.

Перш за все, необхідно зазначити, що відповідно до ст.ст. 51, 55, 56 Регламенту, діяльність вказаних органів поширюється лише на теритеорію держав-членів. Однак, регуляторні дії можуть вплинути на обробку, яка відбувається в інших державах-членах. Такий сценарій можливий у т. зв. 'One-Stop-Shop' випадках, коли:

а) коли компанія здійснює транскордонну діяльність з обробки, і бізнес має кілька установ у ЄС;

б) коли компанія має лише одну установу в ЄС, але обробляє персональні дані жителів більш ніж однієї держави-члена ЄС.

В такому випадку, для того, щоб отримати право на єдине вікно (підпорядковуватись єдиному органу захисту даних, а не кільком), організація повинна мати «головне місце представництва» в ЄС (тобто штаб-квартиру для її діяльності в ЄС або місце, де вона приймає рішення щодо обробки діяльності в ЄС). Якщо така організація не має головного представництва в ЄС, вона не матиме права на єдине вікно та натомість продовжуватиме працювати з DPA кожної держави-члена, у якій вона працює.

Так, у листопаді 2020 року EDPB (Європейська рада із захисту даних) прийняла своє перше рішення за статтею 65 Регламенту після того, як зацікавлені DPA висунули заперечення щодо рішення, прийнятого Ірландською комісією із захисту даних (DPC), яка виконує функції LSA (основного органу захисту даних по відношенню до компанії Twitter в ЄС) по відношенню до компанії Twitter International. Згодом ірландський DPC (DPA) оголосив про своє остаточне рішення в грудні 2020 року, виписавши штраф у розмірі 450 000 євро [15] для компанії Twitter за недотримання вимог щодо сповіщення про порушення даних і ведення записів GDPR – тобто виступив основним органом щодо захисту персональних даних по відношенню до сервісу соціальних мереж, рішення якого вплинуло на практику щодо сповіщення про порушення даних компанією Twitter в інших державах-членах ЄС.

Відповідно до статей 55, 57 Регламенту, національні органи з захисту персональних даних наділені наступними повноваженнями: моніторинг та забезпечення дотримання Регламенту; заслуховування претензій суб'єктів даних або їх представників та їх інформування про результати розгляду відповідних претензій, встановлення вимог до оцінки впливу на захист даних (Impact Assessment). Так, оцінка впливу на захист даних повинна проводитися завжди, коли обробка може призвести до високого ризику для прав і свобод фізичних осіб. Оцінку необхідно проводити особливо, якщо один із прикладів правил, викладених у ст. 35(3) GDPR є актуальним – наприклад, профілювання в соціальних мережах.

До повноважень також відносяться заохочення створення Кодексів поведінки та перегляд сертифікації (типових положень); ведення обліку санкцій та примусових заходів, а також «виконання будь-яких інших завдань, спрямованих на захист персональних даних». Прикладом таких кодексів поведінки є рекомендації 8/2020 щодо орієнтації на користувачів соціальних мереж [16]. Націлювання на користувачів соціальних медіа може включати низку різних суб'єктів, які, для цілей цих рекомендацій, мають бути розділені на чотири групи: постачальники соціальних медіа, їхні користувачі, цільові особи та інші суб'єкти, які можуть бути залучені до процесу націлювання. Важливість правильного визначення ролей і обов'язків різних учасників була підкреслена в рішеннях у справах Wirtschaftsakademie і Fashion ID Суду Європейського Союзу (CJEU) [17]. Обидва рішення демонструють, що взаємодія між провайдерами соціальних мереж і інші учасники можуть нести спільну відповідальність згідно з законодавством ЄС про захист даних. Основна мета цих вказівок полягає в роз'ясненні ролі та обов'язків між постачальником соціальних медіа та цільовою особою. Для цього в настановах також визначаються потенційні ризики для прав і свобод осіб (розділ 3), основні учасники та їхні ролі (розділ 4), а також розглядається застосування ключових вимог захисту даних (таких як законність і прозорість, DPIA тощо), а також ключові елементи домовленостей між постачальниками соціальних медіа та цільовими особами.

Окрім вказаних вище повноважень, сюди, відповідно до положень статті 58 Регламенту, належить право щодо нагляду за дотриманням Регламенту, розслідування порушень Регламенту, а також, за необхідності, порушення судових справ. Наприклад, 11 вересня 2015 року бельгійський DPA подав позов до суду першої інстанції Брюсселя, Бельгія, вимагаючи судової заборони проти Facebook Ireland, Facebook Inc. і Facebook Belgium [18]. Вказані дії мали на меті припинення того, що бельгійське DPA охарактеризувало «серйозним та широкомасштабним порушенням компанією Facebook законодавства щодо конфіденційності». Шостого лютого 2018 року суд першої інстанції

постановив, що соціальна мережа Facebook не належним чином інформувала бельгійських користувачів Інтернету про збір і використання відповідної інформації. Крім того, згода користувачів Інтернету на збір і обробку цих даних була визнана недійсною. Проте Facebook Ireland, Facebook Inc. і Facebook Belgium оскаржили це рішення в Апеляційному суді Брюсселя.

В межах статті 59, вказані органи також зобов'язані щорічно публічно звітувати про виконання покладених на них обов'язків. Відповідна інформація з'являється на сайті кожного національного органу з захисту персональних даних щороку в доступній для користувача формі, яка дозволяє зрозуміти реальну статистику порушень Регламенту в тій чи іншій державі-члені ЄС та вибудувати ефективний план дій на наступний звітний період – так, 7 травня Управління із захисту даних Нідерландів (Dutch DPA) опублікувало свій річний звіт за 2022 рік і річний план за 2023 рік. У 2023 році DPA Нідерландів зосередилось на алгоритмах і штучному інтелекті, великих технологіях, свободі та безпеці [19]. У 2023 році DPA Нідерландів особливо прагнуло забезпечити виправданий баланс між свободою та безпекою обробки персональних даних. Зокрема, нідерландське DPA заявило, що всі розслідування з цього приводу буде завершено в 2023 році і що особливу увагу буде приділено видачі дозволів на обробку персональних даних у кримінальних розслідуваннях. В 2024 році очікується наступний звіт стосовно виконання поставлених завдань.

Стаття 61, 62 надає можливість національних органам з захисту персональних даних здійснювати спільне розслідування та кооперацію задля розслідування порушень Регламенту. Так, ще в 2013 році було проведене спільне розслідування, Управлінням з питань захисту прав Нідерландів та Управлінням уповноваженого з питань конфіденційності в Канаді [20]. У наказі, оскарженому проти Whatsapp, вважалося, що воно порушує законодавчу вимогу до компаній, що не входять до ЄЕЗ, які обробляють персональні дані в Нідерландах, щодо призначення «місцевого представника». Без визначеного представника в Нідерландах, національне нідерландське DPA не могло б ефективно розглядати та контролювати дії компанії Whatsapp.

Наступна частина статті демонструє приклади діяльності національних органів з захисту персональних даних в межах сфери соціальних мереж.

Як зазначено вище, практика національних органів має значний вплив на діяльність соціальних мереж у ЄС та захист конфіденційності їхніх користувачів.

Управління із захисту даних Ірландії (IE DPA) наклало адміністративний штраф у розмірі 1,2 мільярда євро [21] на материнську компанію Facebook Meta за порушення Загального регламенту захисту даних (GDPR) після того, як Meta передала дані європейських користувачів Facebook у США. Технічно штраф було накладено на ірландську дочірню компанію Meta Platforms Inc. Meta Platforms Ireland Limited, але оскільки штраф базувався на загальному глобальному обороті Meta, доречно посилатися на Meta в цілому. Адміністративний штраф був накладений згідно зі статтею 84 GDPR після того, як влада визнала Meta порушенням статті 44 GDPR під час передачі даних користувачів Facebook з Європи до Сполучених Штатів. Штраф є найбільшою адміністративною санкцією, накладеною органами ЄС за порушення GDPR. На суворість штрафу вплинув, серед іншого, той факт, що влада вважала Meta діяла навмисно або принаймні недбало відповідно до статті 83(2)(b) GDPR. Інші сприяючі фактори включали велику кількість переданих персональних даних, велику кількість суб'єктів даних і тривалість порушення [22].

Наступний випадок виник у контексті захисту приватності дітей у соціальних мережах. Зазначені заходи були введені після смерті дитини, яка випадково покінчила з собою, коли ймовірно намагалася взяти участь у «Blackout challenge» на TikTok. Наглядовий орган із захисту даних в Італії видав два тимчасові заходи, які обмежують можливості соціальної медіа-платформи TikTok обробляти дані користувачів, які проживають в Італії, чий вік неможливо визначити з точністю [23]. Наглядовий орган видав два рішення: 2021/20, 22 січня 2021 року; та 2021/61, 11 лютого 2021 року.

У заході 2021/20 DPA Італії наклало на TikTok тимчасове обмеження на обробку персональних даних користувачів, які проживають на території Італії, чий вік неможливо точно визначити. Хоча цей захід був попереднім, це обмеження набуло чинності негайно (за умови подальшої оцінки, проведеної DPA) і діяло до 15 лютого 2021 року.

DPA взяв до уваги, що TikTok ще не надав письмову відповідь на заяву SA в грудні, і підкреслив, що проведене попереднє розслідування виявило серйозні недоліки щодо процедури перевірки віку, прийнятої компанією. SA спеціально посилався на три положення, які підкреслювали важливість захисту інтересів дітей. Він посилався на статтю 24(2) Хартії основоположних прав

Європейського Союзу («Права дитини»), яка зазначає, що «усі дії, що стосуються дітей, незалежно від того, здійснюються вони органами державної влади чи приватними установами. найкращі інтереси дитини мають бути першочерговою увагою». Він також посилався на пункт 38 GDPR, який встановлює, що щодо персональних даних «діти заслуговують на особливий захист», оскільки вони «можуть бути менш обізнаними про ризики, наслідки та відповідні гарантії та свої права щодо обробки даних». особисті дані». У пункті 38 зазначається, що обробка персональних даних дітей має бути спеціально захищена для «цілей маркетингу або створення особистих профілів або профілів користувачів і збору персональних даних щодо дітей під час використання послуг, які пропонуються безпосередньо дитині».

У другому заході DPA зазначив, що оскільки сповіщення, які TikTok надсилає для перевірки віку користувачів, з'явилися лише за три дні до цього, на цьому етапі неможливо було оцінити, чи прийнятий TikTok захід був відповідним та ефективним. Відповідно, воно продовжило дію обмеження, встановленого першим заходом, до 15 березня 2021 року.

Наступний випадок є прикладом порушення конфіденційності, коли провайдер соціальних медіа збирав і зберігав особисті дані щодо контактів своїх учасників з метою надсилання запрошень підключитися на платформі.

19 травня 2020 року Управління із захисту даних Бельгії («Belgian DPA») оголосило, що Судова палата наклала штраф у розмірі 50 000 євро на постачальника соціальних мереж за незаконну обробку персональних даних у зв'язку з «запрошенням друга». », що пропонується на його платформі [24].

У своєму рішенні Судова палата нагадала, що згода повинна бути надана самим суб'єктом даних (за винятком певних ситуацій, наприклад, з неповнолітніми). Таким чином, постачальник соціальних медіа не міг покладатися на згоду, отриману від своїх учасників, для того щоб узаконити обробку персональних даних контактів, які не були учасниками платформи, і, таким чином, ніколи не погоджувалися на обробку їх контактної інформації. Стосовно контактів, які є членами платформи, Судова палата вказала, що, принаймні на початку процесу, користувачам були представлені попередньо вибрані вікна на етапі, де вони могли запрошувати контакти. Судова палата підкреслила, що згода, отримана через попередньо вибрані вікна, не відповідає стандарту дійсної згоди відповідно до GDPR. Що стосується дійсності згоди, Судова палата також зазначила у своєму рішенні, що практика надсилання початкового нерекламного електронного листа для отримання згоди особи на отримання електронного маркетингу не відповідає вимогам GDPR.

Висновки. Проаналізувавши практику діяльності національних органів з захисту персональних даних в ЄС, ми можемо зробити наступні висновки:

1) Для запровадження функціонування вказаних органів необхідним є не лише доповнення, а й розробка цілком нового законодавства про захист персональних даних, яке повинно включати в себе норму про необхідність запровадження відповідного органу в державі, перелік його повноважень, порядок визначення головного контролюючого органу у відносинах, пов'язаних з обробкою суб'єктів даних закордоном та створення умов, необхідних для співпраці відповідних органів як з іншими національними, так і іноземними відповідними установами;

2) Для забезпечення ефективності функціонування вказаних органів, їх рішення не повинні обмежуватись лише рекомендаційним характером. Як бачимо з рішень, прийнятих по відношенню до сервісів соціальних мереж в Бельгії, Італії та Ірландії, можливість швидкого і професійного розслідування та можливість оперативного вжиття запобіжних заходів як і накладення штрафів чи інших санкцій за порушення Регламенту створює позитивну практику для користувачів соціальних мереж. Вказана практика може мати вплив і на функціонування сервісів соціальних мереж поза юрисдикцією держави-члена, оскільки рішення може бути прийняте в режимі 'One-Stop-Shop';

3) Порядок захисту приватності та персональних даних вказаними органами є загальним (універсальним) по відношенню до сфери соціальних мереж. Це означає, що в межах вказаних органів не існує окремих віддлів чи департаментів, які б спеціалізувались на розслідуванні та вжитті заходів щодо порушення Регламенту саме в сфері соціальних мереж – натомість застосовується загальний універсальний порядок розслідування вказаних випадків, який може відбуватись у співпраці з відповідними органами кібербезпеки;

4) Описана практика вказує на необхідність створення окремого органу з захисту персональних даних в Україні, який зможе ефективно впливати на функціонування соціальних мереж в

Україні і тим самим створювати сприятливе для забезпечення безпеки персональних даних середовище. З цією метою необхідно здійснити перегляд ефективності функціонування Уповноваженого Верховної Ради України з прав людини в даній сфері та розглянути можливість покладення вказаних функцій на окремий орган. Зокрема, варто переглянути положення Закону України «Про захист персональних даних» на предмет його відповідності вимогам Загального регламенту даних відповідно до нормативних вимог Угоди про асоціацію з ЄС, який був прийнятий та набув чинності через вісім років після прийняття закону, який діє в Україні та, як мінімум, внести відповідні зміни що стосуються виконання положень ст.ст.51-54 Регламенту в частині створення незалежного наглядового органу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент захисту даних).
2. Директива 95/46/ЄС Європейського Парламенту та Ради від 24 жовтня 1995 р. про захист осіб у зв'язку з обробкою персональних даних і про вільне переміщення таких даних.
3. Міністерство Юстиції України, Державна служба України з питань захисту персональних даних. URL: https://minjust.gov.ua/str_minkoord_zpd.
4. Центр демократії і верховенства права. «Уряд ліквідував Державну службу з питань захисту персональних даних», 17 вересня 2014 року. URL: https://cedem.org.ua/news/uryad-likviduvav-derzhavnu-sluzhbu-z-pyt/.
5. Закон України «Про захист персональних даних», № 2297-VI від 01.06.2010, URL:: https://zakon.rada.gov.ua/laws/card/2297-17.
6. Офіційний веб-сайт Європейського Союзу, Посібник із захисту даних, за адресою: https://edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en.
7. Наім А. Наваз, Кашіф Ісхак, Узма Фарук, Амна Халіл, Саїм Рашид, Аднан Абід і Фадхіла Росді, "Комплексний огляд загроз безпеці та рішень для індустрії соціальних мереж онлайн, 16 січня 2023 р.
8. AIN.UA, «28 млн в YouTube, 10 млн у TikTok: як війна змінила українські соцмережі», 6 серпня 2022 року, URL:: https://ain.ua/2022/08/06/yak-vijna-zminyla-soczmerezhi/.
9. Українська Гельсінська спілка з прав людини, «Що загрожує персональній інформації та правам користувачів у соціальних мережах», 29.11.2023, URL: https://www.helsinki.org.ua/articles/ shcho-zahrozhuie-personalniy-informatsii-ta-pravam-korystuvachiv-u-sotsialnykh-merezhakh-poiasnennia-iurysta/.
10. Робоча група із захисту даних, Рекомендації щодо ідентифікації контролера або провідного наглядового органу, що здійснює обробку даних, прийнято 13 грудня 2016 року, востаннє переглянуто та прийнято 5 квітня 2017 року.
11. Рекомендації ОБСЄ щодо транскордонного співробітництва у забезпеченні виконання законів, що захищають конфіденційність, з https://edps.europa.eu/sites/edp/files/ publication/oecd_guidelines_en.pdf.
12. Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи щодо високого загального рівня кібербезпеки в Союзі, яка вносить зміни до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972, та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2).
13. Федеральний закон про захист даних від 30 червня 2017 року (Вісник федеральних законів I, стор. 2097), з останніми поправками, внесеними статтею 10 Закону від 23 червня 2021 року (Вісник федеральних законів I, стор. 1858; 2022 I, стор. 1045) з https ://www.gesetze-im-internet.de/englisch_bdsg/.
14. Закон Республіки Польща від 10 травня 2018 р. про захист персональних даних, Закон 2018 рік 1000.
15. Європейська рада із захисту даних, Ірландська комісія із захисту даних оголошує рішення щодо запиту у Twitter.
16. Європейська рада із захисту даних, Рекомендації 8/2020 щодо націлювання на користувачів соціальних мереж, 13 квітня 2021 р.

17. Суд Європейського Союзу, прес-реліз № 99/19. Люксембург, 29 липня 2019 р. Рішення у справі C-40/17, Fashion ID GmbH & Co. KG проти Verbraucherzentrale NRW.
18. Бельгійський національний орган з захисту персональних даних, «Орган із захисту даних захищає свої аргументи перед Апеляційним судом у Брюсселі у справі Facebook», з https://www.dataprotectionauthority.be/citizen/the-authority/organisation.
19. Управління із захисту даних Нідерландів, звіт про ризики ШІ та алгоритмів, Нідерланди – зима 2023–2024 рр., 18 січня 2024 р.
20. CBC News, WhatsApp порушує закони про конфіденційність, 28 січня 2013 р., з https://www.cbc.ca/news/science/whatsapp-breaches-privacy-laws-1.1343435.
21. Європейська рада із захисту даних, «1,2 мільярда євро штрафу для Facebook у результаті обов'язкового рішення EDPB», 22 травня 2023 р.
22. Скурнік Т., Майбутня передача персональних даних за межі ЄС, Закон Nordia, 29.05.2023, з https://nordialaw.com/insights-data-privacy/.
23. Колумбійський університет, Управління із захисту даних Італії проти TikTok, аналіз справи, з https://globalfreedomofexpression.columbia.edu/ cases/italian-data-protection-authority-v-tiktok/.
24. Блог законів про конфіденційність та інформаційну безпеку, Оновлення та аналіз глобального законодавства про конфіденційність і кібербезпеку, Бельгійське DPA накладає санкції на компанію соціальних мереж за незаконну обробку персональних даних у зв'язку з функцією «Запросити друга», 27 травня 2020 р.