УДК 343.45

Гронь О. В.
кандидат економічних наук, доцент,
доцент кафедри міжнародного бізнесу та економічного аналізу
Харківського національного економічного університету
імені Семена Кузнеця
Погореленко А. К.
студентка факультету консалтингу і міжнародного бізнесу
Харківського національного економічного університету
імені Семена Кузнеця

Gron` O. V.
PhD in Economics, Associate Professor,
Associate Professor of the Department
of International Business and Economic Analysis
Simon Kuznets Kharkiv National University of Economics
Pohorelenko A. K.
First year student, Faculty of consulting and international business
Simon Kuznets Kharkiv National University of Economics

ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У КОНТЕКСТІ СУЧАСНОЇ КОМУНІКАЦІЇ

Анотація. У статті проаналізовано європейські законодавчі основи та принципи захисту персональних даних, які становлять основу сучасної практики в цій сфері. Викладено базові положення української системи правового захисту персональних даних. Визначено правові підстави для реалізації та захисту інтересів суб'єкта персональних даних. Окреслено подальші напрями вдосконалення системи захисту персональних даних.

Ключові слова: персональні дані, комунікація, ідентифікація, захист, інформація, втручання, правове забезпечення, регулювання, механізм.

Постановка проблеми. Завдяки стрімкому розвитку інформаційних технологій доступ до різноманітних каналів комунікації отримали не лише організації та корпорації, але й окремі особи. У сучасний період кожна людина має можливість створювати свої власні повідомлення та поширювати інформацію, яка буде доступна необмеженій кількості користувачів. У результаті масового і неконтрольованого доступу усіх членів суспільства до інформаційно-комунікаційних технологій приватна «завіса», яка ще донедавна дозволяла «ховати» значний масив особистої інформації від сторонніх, була скинута. Як наслідок, відбулася низка інформаційних скандалів, які привернули увагу суспільства до проблеми захисту персональної інформації та спричинили широкомасштабне обговорювання цієї проблеми. Першою «ластівкою» у 2010 році став скандал з Wikilieaks, яка надала доступ у Всесвітній мережі до таємної інформації щодо дипломатичного листування США. У результаті скандалу у 2013 році, пов'язаного з колишнім співробітником Агентства національної безпеки США Едвардом Сноуденом, світ дізнався про стеження за користувачами інтернету через прослуховування телефонних розмов та контролювання листування американськими та британськими спецслужбами. У 2016 році відбувся черговий виток інформації, який отримав назву «Panama Papers», він пролив світло на приховування доходів та ухилення від сплати податків відомими світовими лідерами та бізнесменами.

Значну увагу суспільства привернула остання подія – онлайн-кампанія британської консалтингової фірми «Cambridge Analytica», за допомогою якої кандидат у Президенти США Дональд Трамп переміг у виборах у 2016 році. В основі методів роботи фірми був несанкціонований доступ до персональних даних 50 мільйонів користувачів соціальної мережі «Facebook» для визначення політичних симпатій виборців для впливу на них через відповідну рекламу та публікації у стрічці новин, які дискредитували Хіларі Клінтон. Американські та європейські законотворці затребували пояснень, яким чином «Cambridge Analytica» отримала доступ до даних та чому соціальна мережа не поінформувала про це своїх користувачів.

Вільний широкий доступ до інформації та можливість продукувати нову інформацію сприяє створенню можливостей та розвитку особистості, але стрімкий розвиток інформаційно-комунікаційних технологій потребує розроблення та впровадження адекватних захисних механізмів, спроможних реально захистити персональні права та свободи власників особистих даних. Незважаючи на значну увагу з боку суспільства та держави до питання захищеності персональних даних від втручання та потенційного оприлюднення сторонніми особами, в сучасних умовах воно й досі залишається відкритим. Все це й зумовлює проблематику та актуальність проведення дослідження та доцільність пов'язаного із дослідженням механізму захисту особистої інформації.

Аналіз останніх досліджень і публікацій. Проблемам захисту особистих даних приділяється сьогодні багато уваги. Вони є дуже значущими як із теоретичної, так і з практичної позиції. Цим дослідженням приділено увагу в наукових працях багатьох учених.

Особливий інтерес до висвітленої проблеми проявляли М.В. Бем, І.М. Городинський, Г. Саттон, О.М. Родіоненко [1], О.Г. Рогова [2], С.С. Єсімов [3], В.О. Волосецький [4], В.М. Брижко [5], К.С. Мельник [6; 7], О.Г. Рогова [8], Т. Обуховська [9], О. Мервінський [10], М. Кравчук [11], Ж.В. Удовенко [12], В.В. Оніщенко [13] та інші вчені.

У своїх працях фахівці приділили багато уваги захисту персональних даних на основі аналізу європейського та вітчизняного законодавства. При цьому в цих працях недостатньо висвітлено проблеми, пов'язані з розробленням базових складників механізму, який був би здатен унеможливити оприлюднення конфіденційної інформації в будь-яких інших джерелах, не передбачених чинними законодавчими нормами.

Метою статті є узагальнення наявних організаційно-правових основ захисту персональних даних у сучасних умовах та розроблення рекомендацій щодо визначення складників відповідного механізму.

Результати дослідження. Захист особистих даних сьогодні – фундаментальне та досить комплексне поняття, яке, з одного боку, відображає прагнення захистити недоторканність особистого життя, з іншого – визначає його як інформацію, яка відображає участь особистості в суспільних та соціальних відносинах, що робить особисте життя доволі уразливим об'єктом щодо отримання особистих даних іншими особами [3]. Воно відображає цілий комплекс дій з отримання та обробки інформації, яка дозволяє ідентифікувати конкретну особу. Інститут захисту персональних даних є елементом державної системи захисту інформації, що забезпечує особисту безпеку, підтримує баланс інтересів особистості, суспільства та держави у сфері обробки інформації [3].

Варто відмітити, що незважаючи на актуальність проблематики щодо захисту персональних даних, теоретична дискусія щодо змісту поняття «захист персональних даних» у науковій літературі відсутня. Дослідження вітчизняних учених зосереджені на опрацюванні та систематизації наявного нормативного поля, яке забезпечує правове врегулювання захисту персональних даних.

Дещо краща ситуація склалася щодо поняття «персональні дані», трактування змісту якого знайшло своє відображення у таких нормативних джерелах (табл. 1).

Аналіз наведених визначень свідчить про те, що в основному вони збігаються, ключовим моментом усіх визначень є можливість безпомилкової ідентифікації конкретної особи.

В основу обробки персональних даних покладено низку базових принципів (правила, що повинні дотримуватися (за незначними винятками) будь-яким володільцем у процесі здійснення будь-якої обробки), мета формулювання яких – визначення правових засад її здійснення. Вони формуються на наднаціональному та національному рівнях.

Ключові принципи у Європейському Союзі були покладені в основу правового захисту персональних даних Директивою 95/46/ЄС [16]. При цьому зміни, які передбачені новим Регламентом [18] про персональні дані, знаменують якісно нову філософію щодо їх охорони із відповідними жорсткими санкціями за порушення його вимог [19].

Так, документом передбачається навіть варіювання видів відповідальності – від штрафів у розмірі до 20 млн євро або 4% від щорічного світового обігу компанії (контролера або обробника) до кримінальної відповідальності (залежно від національного законодавства).

Україна, яка поступово інтегрується до ЄС, вже має відповідні базові положення, спрямовані на створення якісної системи правового захисту персональних даних.

Конституцією України [20] (стаття 32) зазначається: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». Саме це – той «базис», спираючись на який «вбудовуються» усі подальші законодавчі норми щодо захисту персональних даних.

Отже, розглянемо практичний (регламентаційний) бік цього питання. В цій частині проаналізуємо ключові нормативні документи, виходячи з того, в який період часу вони були прийняті. Це, на думку авторів, – особливий складник досліджуваного процесу, оскільки під законодавче врегулювання тут підпадають доволі «вразливі» дані про особу (майновий стан, політичні уподобання, релігійна приналежність, ідентифікаційний податковий номер та інші дані). Тому й відповідні механізми повинні бути максимально виваженими та коректними, аби за-

Таблиця 1

Нормативне визначення поняття «персональні дані»

Нормативний акт	Зміст поняття
Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року (дата ратифікації Україною: 06.07.2010 року, дата набрання чинності для України: 01.01.2011 року) [14]	Персональні дані – будь-яка інформація, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною.
Закон України «Про інформацію» від 02.10.1992 року № 2657-XIII [15]	Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.
Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року [16]	Персональні дані означають будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити («суб'єкт даних»). Особою, яку можна встановити, є така, яка може бути встановленою прямо чи непрямо, зокрема, за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості.
Закон України «Про захист персональних даних» від 1.06.2010 року № 2297-VI [17]	Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.
Загальне положення про захист даних / EU General Data Protection Regulation (GDPR) [18] (набуває чинності з 25 травня 2018 року)	Персональні дані – вся інформація, що стосується особи, за якою її прямо чи опосередковано можна ідентифікувати.

Джерело: [14; 15; 16; 17; 18]

хистити дані від злочинців або аферистів. Саме викладена нижче календарна послідовність ілюструє розвиток системи обробки та захисту інформації та включає в себе не тільки українські законодавчі ініціативи, а й європейські, які вже апріорі «вбудовуються» у вітчизняну практику.

1. Базовий в Україні нормативний документ з цього питання – Закон України «Про захист персональних даних» (набрав чинності з 1 січня 2011 року) [17]. Він регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

Статтею 6 «Загальні вимоги до обробки персональних даних» передбачено:

– мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних;

– персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх обробки;

– склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки;

– первинними джерелами відомостей про фізичну особу є: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.

– обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством;

– не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини;

– якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим;

– персональні дані обробляються 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;

– типовий порядок обробки персональних даних затверджується Уповноваженим Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних.

Правники характеризують цей Закон як не досить досконалий у зв'язку з відсутністю диференціації персональних даних на вразливі (до яких встановлюються додаткові заходи щодо забезпечення безпеки: расове походження; політичні, світоглядні та релігійні уподобання, здоров'я, біометричні та генетичні дані та ін., обробка яких здійснюється в спеціальному порядку, який регламентується окремо) та звичайні, як це має місце у міжнародних документах. Причина: доволі багато фахівців із безпеки допускають масове негласне спостереження, але винятково в межах державної таємниці та забезпечення чіткого балансу між захистом персональних даних та забезпеченням національної безпеки в епоху після 11 вересня 2001 року [21].

2. Прагнення законотворців запровадити європейські підходи до захисту прав людини проявились у прийнятті низки коригувань. Серед них – Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [22] (набув чинності з 1 січня 2014 року), який запровадив функцію контролю за додержанням законодавства про захист персональних даних на Уповноваженого Верховної Ради України з прав людини [23]. З цією метою в Секретаріаті Уповноваженого Верхової Ради України з прав людини створено Департамент із питань захисту персональних даних [24], ключовою функцією якого задекларовано «моніторинг дотримання прав людини у сфері захисту персональних даних».

3. Ширший, ніж досліджуване питання, та дуже суттєвий за своїм змістом документ – Закон України «Про доступ до публічної інформації» [25], внесені зміни у 2015 році до якого ознаменували собою певну реформу доступу до публічної інформації та ведення відкритих даних, відповідно до яких:

– персональні дані знеособлені та захищені відповідно до Закону Україні «Про захист персональних даних» [17];

– фізичні особи (суб'єкти даних), персональні дані яких містяться в інформації у формі відкритих даних, надали свою згоду на поширення таких даних відповідно до Закону України «Про захист персональних даних» [17];

– надання чи оприлюднення такої інформації передбачено законом;

– обмеження доступу до такої інформації (віднесення її до інформації з обмеженим доступом) заборонено законом.

4. Визначені вище інформаційні скандали спричинили відповідну реакцію європейських регуляторів. Так, рекомендація CM/Rec (2016)5 Комітету Міністрів державам – членам від 13 квітня 2016 року «Щодо Інтернет-свободи» [26] (набрала чинності з 13 квітня 2016 року) вказує на те, що Інтернет-свобода розуміється як реалізація і користування в Інтернеті правами людини і основоположними свободами, а також їх захист відповідно до Європейської конвенції про захист прав людини і основоположних свобод та Міжнародного пакту про громадянські і політичні права.

Документом вказується, що інтернет-свобода базується насамперед на праві на свободу слова, праві на свободу зібрань та об'єднання, праві на приватне життя і праві на ефективний засіб юридичного захисту. Тому і відповідні механізми управління інтернетом на усіх рівнях (глобальному, національному, регіональному) повинні ґрунтуватися на цих базових правах людини. Здійснення державою своїх суверенних прав повинно враховувати ці міжнародні норми та утримуватись від дій, які прямо чи опосередковано можуть завдати шкоди фізичним або юридичним особам в межах або за межами їх юрисдикції.

Документом рекомендується проводити регулярну оцінку ситуації щодо Інтернет-свободи на національному рівні. З цією метою документом рекомендується:

– періодично оцінювати рівень дотримання та імплементації прав людини і основних стандартів Інтернет-свободи;

– забезпечити участь усіх зацікавлених сторін із приватного сектору, громадянського суспільства, наукових кіл та технічної спільноти в оцінці стану Інтернет-свободи та підготовці відповідних досліджень;

– спільно використовувати отримані результати.

5. Наступний документ – регламент (Євросоюз) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [27] (набирає чинності з 25 травня 2018 року). Він спрямований на «гармонізацію захисту основних прав і свобод фізичних осіб щодо діяльності з переробки і на забезпечення вільного потоку персональних даних між державами-членами».

Регламент покликаний сприяти розбудові простору свободи, безпеки, справедливості і економічного союзу; економічного і соціального прогресу; зміцненню законності і зближення економік в межах внутрішнього ринку, а також загальному добробуту фізичних осіб держав-членів.

Документом передбачаються відповідні повноваження для моніторингу та забезпечення дотримання правил захисту персональних даних та санкції за їх порушення в державах-членах. Зокрема, документом зазначається, що обробка персональних даних (ОПД) є законною тільки в тому разі і в тій мірі, в якій виконується щонайменше одна з таких умов:

– суб'єкт персональних даних дав згоду на обробку своїх персональних даних для однієї чи кількох конкретних цілей;

– ОПД є необхідною для виконання договору, в якому суб'єкт даних є стороною або з метою вжиття заходів на прохання суб'єкта даних для укладення договору;

– ОПД є необхідною для відповідності юридичним зобов'язанням, покладеним на контролера;

– ОПД є необхідною для захисту важливих інтересів суб'єкта, його даних або іншої фізичної особи;

– ОПД є необхідною для виконання поставленого завдання, що проводиться в інтересах суспільства або під час виконання службових обов'язків, покладених на контролерів;

– ОПД є необхідною для цілей захисту законних інтересів, які переслідує контролер або третя сторона, за винятком випадків, коли такі інтереси перекриваються інтересами основоположних прав і свобод суб'єкта даних, який потребує захисту персональних даних, зокрема, коли суб'єктом даних є дитина.

Передбачено також, що якщо ОПД є необхідною для інших цілей, необхідно встановлювати сумісність мети такої обробки з цілями, для яких було зібрані персональні дані, а також передбачати наступну адміністративну відповідальність, яка визначатиметься компетентним органом [23].

На підставі викладеного очевидно, що персональні дані обробляються на підставі згоди особи та на підставі положень відповідних законів і нормативних актів. Щоб відповідати закону, згода повинна володіти ознаками добровільності (відсутність примусу під час її надання), поінформованості (чітке розуміння про те, ким та з якою метою будуть оброблятися персональні дані) та зовнішньої форми (будь-яка неписьмова форма надання персональних даних, з якою погоджується особа, дані якої обробляються) [1]. Ключовий момент у цьому – саме те, наскільки захищена надана персональна інформація та наскільки ймовірна можливість припинення її обробки.

Різноманітні комунікаційні канали стали частиною повсякденного життя значної кількості людей, але небагато хто з них переймається безпекою персональних даних, надаваних у процесі комунікації. Стикаючись із випадками агресивної маркетингової поведінки шляхом розсилки e-mail або sms-повідомлень про рекламні акції, надаючи купу довідок до різних установ, споживачі іноді навіть не замислюються про порушення компаніями й організаціями законодавства щодо захисту персональних даних. Юристи кажуть, що правових підстав, зафіксованих у національному законодавстві, для обробки у приватно-правових володільців персональних даних інших осіб нема, тому особа має повне право вимагати припинити таку обробку в цілях реалізації непотрібних їм інтересів.

Головне в процесі збору, зберігання та обробки даних – захист прав і свобод людини щодо:

– невтручання в особисте життя під час обробки персональних даних;

– необхідності обробки лише в цілях законних інтересів, переслідуваних контролером чи третьою стороною або сторонами, для яких надаються дані, крім випадків, коли над такими інтересами переважають інтереси основних прав і свобод суб'єкта даних.

Саме це і є та правова підстава, яка не тільки реалізує, а й захищає законні інтереси суб'єкта персональних даних. Для того щоб відстоювати свої права, згідно із Законом України «Про захист персональних даних» від 1.06.2010 року № 2297-VI [17], суб'єкт персональних даних повинен мати чітке уявлення про:

– мету збору персональних даних (має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних);

– володільця персональних даних (фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом);

– розпорядника персональних даних (фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця);

– склад та зміст персональних даних (мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки).

Окремий складник обізнаності суб'єкта персональних даних – свої права. Так, статтею 8 Закону передбачено такі права суб'єкта персональних даних:

– знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних;

– отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

– на доступ до своїх персональних даних;

– отримувати не пізніше, як за тридцять календарних днів із дня надходження запиту (крім випадків, передбачених законом), відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

– пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

– пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

– на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

– звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

– застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

– вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

– відкликати згоду на обробку персональних даних; знати механізм автоматичної обробки персональних даних;

– на захист від автоматизованого рішення, яке має для нього правові наслідки.

Досконале знання цих прав дозволяє обґрунтовано та якісно відстоювати свої інтереси у разі, коли персональна інформація стає відомою стороннім особам, тоді, коли це не пов'язано із питаннями державної та громадської безпеки, боротьби з злочинністю, запобіганню правопорушенням та ін.

Реалізація цієї значущості підтверджується значною увагою до цих питань у щорічній доповіді [28] Уповноваженого Верховної Ради України (розділ 8 «Дотримання права на захист персональних даних»). У доповіді за 2017 рік зазначається, що «Управлінням із питань захисту персональних даних Секретаріату Уповноваженого було розглянуто 1211 звернень (скарг) фізичних та юридичних осіб з питань, пов'язаних із захистом персональних даних, в тому числі щодо надання роз'яснень про застосування окремих положень Закону України «Про захист персональних даних». За результатами перевірок було видано та передано для обов'язкового виконання 38 приписів про усунення порушення вимог законодавства у сфері захисту персональних даних, виявлених під час перевірки». Уповноважений справедливо вважає, що, «аналізуючи звернення громадян, а також результати здійснених заходів контролю у сфері захисту персональних даних, можна констатувати, що у 2017 році ситуація у сфері права на приватність залишається незмінною. Недотримання законодавства про захист персональних даних, його нерозуміння та неправильне застосування, як і в попередні роки, залишаються основними підставами, що призводять до порушення права суб'єктів персональних даних на доступ до своїх персональних даних, незаконного поширення персональних даних тощо».

До низки проблемних питань, пов'язаних з організацією процесів обробки персональних даних, Уповноважений відносить [28]:

– невідповідність внутрішніх положень/документів володільця персональних даних вимогам чинного законодавства про захист персональних даних;

– неналежне ведення обліку операцій, пов'язаних з обробкою персональних даних та доступом до них;

– недотримання принципу строковості обробки персональних даних;

– відсутність плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;

– відсутність зобов'язання про нерозголошення персональних даних працівниками, які мають доступ до персональних даних;

– неповідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, та про створення (визначення) відповідального структурного підрозділу або відповідальної особи, що організовує роботу, пов'язану із захистом персональних даних при їх обробці».

Безпека особистих даних – поняття, яке залежить не тільки від норм, прописаних в Законах та нормативних джерелах. Вирішувати його треба ґрунтовно й послідовно, а не лише в момент «витоку» інформації, який призвів до негативних наслідків. Ігнорування потенційних ризиків доти, доки не трапиться найгірше, є не найкращою стратегією.

Знаковий для цього крок [29] – початок дії у ЄС з 25 травня 2018 року нового Закону про захист конфіденційних даних. GDPR (General Data Protection Regulation, або Загальне положення про захист даних) – новий закон Європейського Союзу про конфіденційність даних, який гармонізує закони про конфіденційність в усьому ЄС і оновлює директиву із захисту даних від 1995 року [16].

Відмітимо, що у ЄС норми Регламенту мають пряму дію та обов'язкові до застосування в усіх державах-членах (порівняно с минулою практикою – коли країни-учасники ЄС могли певним чином обирати між ними та національними нормами, імплементованими під європейські).

Так, новим документом, зокрема, передбачається:

– демонстрація (доведення) відповідності вимогам GDPR;

– підвищення рівня безпеки персональних даних;

– запровадження контролю за передачею персональних даних за межі Європейського економічного простору;

– обмеження можливості використання хмарних сховищ для розміщення персональних даних;

– загальне підвищення рівня приватності;

– вдосконалена процедура повідомлення про витік даних;

– зміцнення контролю у відносинах між контролерами та обробниками;

– обмеження можливості залучення субобробників;

Серед основних прав, які були вдосконалені Регламентом, варто виділити такі:

1. Право бути поінформованим. Якщо інформація збирається безпосередньо від індивіда, необхідним є його оповіщення про це та отримання однозначної згоди. Згода повинна бути відкритою, явно вираженою та незавуальованою (наприклад, на практиці може виражатися як проставляння галочки біля кожного пункту персональних даних, що вводяться у мобільному додатку виклику таксі). Згода не може бути мовчазною та повинна бути відділена від інших умов договору (в тому числі приєднання як terms and conditions в соціальних мережах).

2. Право на видалення (право бути забутим). За запитом суб'єкта, вся інформація про нього повинна бути видалена. Цього правила можна не дотримуватися, якщо інформація необхідна для реалізації права на інформацію, виконання норм чинного законодавства, забезпечення громадського здоров'я, наукової, історичної чи статистичної мети, вирішення правових спорів. Компанії, які можуть розміщувати інформацію користувачів онлайн, повинні за запитом особи видаляти не лише інформацію, а й посилання на неї чи будь-які можливі копії.

3. Право на заборону обробки. Компанія зобов'язана відмовитися від обробки персональних даних на вимогу суб'єкта. Методами, за допомогою яких компанія може це здійснити, є унеможливлення доступу третіх осіб до даних, видалення їх із веб-сайту тощо.

Дуже важливим в цьому є, з одного боку, узгоджена робота фахівців із безпеки, до компетенції яких безпосередньо відноситься це питання, а також IT-фахівців, які розробляють відповідне програмне забезпечення, обов'язкова опція якого – неможливість попадання персональних даних до сторонніх осіб.

Аналітики [30] кажуть, що сьогодні для організації повноцінної системи безпеки даних не вистачає фахівців (у зв'язку з тим, що кращі кадри виїжджають на працю за кордон). Але питання безпеки персональних даних потребує значної уваги та залучення до цього компетентних спеціалістів, оскільки інформаційне поле – дуже незахищене «місце» серед усіх напрямів особистого (чи підприємницького) простору. Відношення до витрат на цей напрям володільців персональних даних певною мірою є перевіркою, яка відображає ступінь їхньої зрілості та реакції на будь-які інформаційні потрясіння.

Перспективами вдосконалення найбільш «слабкої ланки» в системі обробки персональних даних – захисту – є:

– юридичне супроводження захисту персональних даних у мережі Internet, оскільки ця незахищеність сьогодні стає вагомим важелем впливу на діяльність суб'єктів персональних даних;

– чітка фіксація відповідальності володільців персональних даних у випадках, коли ці дані стають загальновідомими (через санкції, притягнення до адміністративної відповідальності та інші).

Дуже важливий момент [19] – відповідність чинних у конкретній компанії процедур із обробки та захисту персональних даних вимогам GDPR. Компанія повинна вдосконалити договори, розроблені всередині своєї структури (трудові чи цивільно-правові) з третіми особами чи партнерами, враховуючи наявне законодавство ЄС.

Поки що не дуже зрозумілими залишаються питання, пов'язані із застосуванням визначених у новому Регламенті [18] видів відповідальності. Залишається лише сподіватися, що відповідний спосіб буде розроблений найближчим часом. Це дозволить додатково врегулювати правовідносини, які пов'язані із найбільш вразливими сьогодні питаннями системи обробки персональних даних – їх захистом.

Висновки. Незважаючи на гучні скандали щодо доступу та оприлюднення персональних даних та зростання критики на адресу соціальних мереж, у щоденному житті користувачі продовжують залишати чимало особистих даних (і не лише в мережі Інтернет), іноді навіть не здогадуючись про можливість використання їх третіми особами. Саме тому контроль за дотриманням правил збору, зберігання та захисту персональної інформації повинні взяти на себе державні органи. Захист персональних даних повинен враховувати усі етапи, що пов'язані з персональними даними, – від їх збирання до знищення або ж втрати ними актуальності.

Базовою метою захисту персональних даних повинно бути забезпечення ключових прав та свобод громадян. Організаційно-економічною «площиною» для її реалізації повинен стати відповідний механізм, в якому основою має бути чинний Закон України «Про захист персональних даних» та в який гармонічно будуть імплементовані ключові європейські норми з чітким визначенням норм щодо свободи інформації та захистом персональних даних, а також деталізацією взаємодії та фіксацією відповідальності за порушення норм у сфері захисту персональних даних.

Список використаних джерел:

1. Бем М.В., Городинський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с. URL: http://er.ucu.edu.ua/bitstream/handle/1/449/Protection%20of%20personal%20data.pdf?sequence=1&isAllowed=y.
2. Рогова О.Г. Захист персональних даних у законодавстві Європейського союзу. URL: http://www.kbuapa.kharkov.ua/e-book/tpdu/2011-3/doc/5/05.pdf.
3. Єсімов С.С. Захист персональних даних у контексті розвитку динамічних систем. Науковий вісник державного університету внутрішніх справ. 2013. № 3. С. 198–207. URL: http://www2.lvduvs.edu.ua/documents_pdf/visnyky/nvsy/03_2013/13yessdis.pdf.
4. Волосецький В.О. Іноземний досвід правового регулювання захисту персональних даних / Міжнародний науковий журнал. URL: https://www.inter-nauka.com/uploads/public/14815322304340.pdf.
5. Брижко В.М. Захист персональних даних: реалії та практика сучасності / Інформація і право. 2013. № 3(9). С. 31–49.
6. Мельник К.С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних / К.С. Мельник // Інформаційна безпека людини, суспільства, держави. 2013. № 2(12). С. 97–103.
7. Мельник К.С. Удосконалення нормативно-правового регулювання захисту персональних даних в Україні / Правова інформатика. 2014. № 1(41). С. 30–44.
8. Рогова О.Г. Захист персональних даних у законодавстві Європейського Союзу та України / Теорія та практика державного управління: зб. наук. пр. Х.: Вид-во ХарРІ НАДУ «Магістр», 2011. Вип. 3 (34). 512 с.
9. Обуховська Т. Класифікація персональних даних та режиму доступу до них // Механізми державного управління. URL: http://visnyk.academy.gov.ua/wp-content/uploads/2013/11/2013-1-13.pdf.
10. Мервінський О. «Чутливі» персональні дані. Як вони захищені? URL: http://yurincom.com/ua/legal_practice/analitychna_yurysprudentsiia/chutlyvi_personalni_dani__yak_vony_zakhyshcheni_-publication/.
11. Кравчук М. Міжнародний досвід правового регулювання захисту персональних даних у мережі Internet. URL: https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwjdtdiG7NXaAhVrD5oKHbIAB9gQFgg5MAI&url=http%3A%2F%2Fwww.irbis-nbuv.gov.ua%2Fcgi-bin%2Firbis_nbuv%2Fcgiirbis_64.exe%3FC21COM%3D2%26I21DBN%3DUJRN%26P21DBN%3DUJRN%26Z21ID%3D%26IMAGE_FILE_DOWNLOAD%3D1%26Image_file_name%3DPDF%2FNzizvru_2013_3_24.pdf&usg=AOvVaw0Q53J0URH5wzvODgHNGYDp.
12. Удовенко Ж.В. Сутність інформації про особисте життя та її види. URL: https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwjdtdiG7NXaAhVrD5oKHbIAB9gQFghMMAQ&url=http%3A%2F%2Fnaukajournal.org%2Findex.php%2FParadigm%2Farticle%2Fdownload%2F285%2F472&usg=AOvVaw1Mse2zCIIHL5nw52kqXLjG.
13. Оніщенко В.В. Захист персональних даних. URL: http://jrnl.nau.edu.ua/index.php/UV/article/viewFile/6540/7311.
14. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року. URL: http://zakon3.rada.gov.ua/laws/show/994_326.
15. Закон України «Про інформацію» від 02.10. 1992 року № 2657-XIII. URL: http://zakon5.rada.gov.ua/laws/show/2657-12.
16. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. URL: http://zakon3.rada.gov.ua/laws/show/994_242.
17. Закон України «Про захист персональних даних» від 1.06.2010 року №2297-VI (зі змінами та доповненнями). URL: http://zakon3.rada.gov.ua/laws/show/2297-17.
18. EU General Data Protection Regulation (GDPR). URL: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.
19. GDPR – нові виклики для обробників персональних даних / К. Тищенко / Юридична газета online. URL: http://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/gdpr--novi-vikliki-dlya-obrobnikiv-personalnih-danih-v-ukrayini.html.
20. Конституція України // Відомості Верховної Ради. 1996. № 30. 141 с.
21. Панамагейт, файли Сноудена та Wikileaks. Найгучніші викриття, які змінили історію. ТСН. Світ. 5 квітня 2016 року. URL: https://tsn.ua/svit/panamageyt-fayli-snoudena-ta-wikileaks-nayguchnishi-vikrittya-yaki-zminili-istoriyu-625101.html.
22. Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» від 03.07.2013 р. № 383-VII. URL: http://zakon4.rada.gov.ua/laws/show/383-18.

23. Уповноважений Верховної Ради з прав людини / Офіційний сайт: http://www.ombudsman.gov.ua/ua/page/zpd/.
24. Департамент з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини / Офіційна сторінка: http://www.ombudsman.gov.ua/ua/page/zpd/info/.
25. Закон України «Про доступ до публічної інформації» від 13 січня 2011 року № 2939-VI. URL: http://zakon2.rada.gov.ua/laws/show/2939-17.
26. Recommendation CM/Rec (2016)5 of the Committee of Ministers to member States on the Internet freedom. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa.
27. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ENм.
28. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина. Київ, 2017. 627 с. URL: http://www.ombudsman.gov.ua/ua/page/secretariat/docs/presentations/&page=3.
29. The Economist: З травня 2018-го у ЄС почне діяти новий закон про захист конфіденційних даних / Тиждень.UA. 5 січня 2018 року. URL: http://tyzhden.ua/News/207156.
30. Бизнес в зоне риска: 5 ошибок при создании службы информационной безопасности. Спецпроект / Новое время. 29 апреля 2018 года. URL: https://nv.ua/ukraine/events/biznes-v-zone-riska-5-oshibok-pri-sozdanii-sluzhby-informatsionnoj-bezopasnosti--2466096.html.

ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В КОНТЕКСТЕ СОВРЕМЕННОЙ КОММУНИКАЦИИ

Аннотация. В статье проанализированы европейские законодательные основы и принципы защиты персональных данных, которые составляют основу современной практики в этой сфере. Изложены базовые положения украинской системы правовой зашиты персональных данных. Определены правовые основания для реализации и защиты интересов субъекта персональных данных. Предложены дальнейшие направления усовершенствования системы защиты персональных данных.

Ключевые слова: персональные данные, идентификация, защита, информация, вмешательство, правовое обеспечение, регулирование, механизм.

PERSONAL DATA PROTECTION PROBLEMS WITHIN THE CONTEXT OF MODERN COMMUNICATIONS

Summary. The article analyzes the European legislative framework and the principles of personal data protection that form the basis of modern practice in this field. The main principles of the Ukrainian system of legal protection of personal data are set out. The legal grounds for implementation and protection of the interests of the subject of personal data are determined. Suggestion for further improvement of the system of personal data protection are offered.

Key words: personal data, identification, protection, information, interference, legal support, regulation, mechanism.