УДК 343.412:341.1:343.9
DOI https://doi.org/10.32782/yuv.v6.2023.36

Є. Полях,
аспірантка відділу кримінологічних досліджень
Науково-дослідного інституту вивчення проблем злочинності
імені академіка В. В. Сташиса Національної академії правових наук України

МОЖЛИВОСТІ ЗАСТОСУВАННЯ МІЖНАРОДНОГО ТА ЗАРУБІЖНОГО ДОСВІДУ ЗАПОБІГАННЯ ПОРУШЕННЯМ НЕДОТОРКАННОСТІ ПРИВАТНОГО ЖИТТЯ У ВІТЧИЗНЯНІЙ ПРЕВЕНТИВНІЙ ПРАКТИЦІ

Постановка проблеми. Порушення недоторканності приватного життя – проблема, від якої потерпає не лише українське суспільство, а і вся світова спільнота. Міжнародні організації та провідні держави світу, усвідомлюючи стрімкі темпи науково-технічного прогресу та його негативний вплив на схоронність персональних даних, розробили власні заходи протидії та запобігання порушенням приватності, у результаті впровадження яких вдалося знизити кількість порушень недоторканності приватного життя. Наразі в Україні поки немає достатньої законодавчої бази і системи заходів, здатної ефективно реагувати на виклики сучасності у вказаній сфері. В питанні захисту персональних даних країна все частіше спирається на міжнародний та зарубіжний досвід, тому дослідження останнього владне визначити необхідні вектори розвитку та сприяти розробці комплексу ефективних заходів запобігання порушенням приватності на теренах нашої держави.

Аналіз останніх досліджень та публікацій. Аналіз міжнародного та зарубіжного досвіду запобігання порушенням недоторканності приватного життя крізь призму охорони та захисту права на персональні дані неодноразово ставав предметом досліджень українських науковців. Зокрема, А. Кардаш, І. Романюк, О. Радкевич у межах своїх дисертаційних досліджень з конституційного та цивільного права приділили достатню увагу цьому питанню, а міжнародні та зарубіжні нормативно-правові акти були предметом досліджень В. Брижка, К. Мельника, Ю. Когута, В. Бєлєнького та багатьох інших науковців. Однак станом на сьогодні більшість з цих праць вже втратили актуальність у зв'язку з прийняттям нових актів, наприклад, Загальний регламент про захист даних (General Data Protection Regulation, далі – GDPR) тощо. Крім того, в українській правовій доктрині відсутні праці за вказаною темою з точки зору кримінології. Останні публікації, присвячені аналізу механізмів захисту приватності у різних країнах світу, простежуються серед закордонних авторів – П. Піттмана (P. Pittman), А. Хафіза (A. Hafiz), А. Хемма (A. Hamm), Т. Хікменна (T. Hickman), Дж. Девіне (J. Devine) та деяких інших, проте логічно, що вони не містять жодних співставлень з правом нашої держави чи рекомендацій щодо модернізації українського правового поля.

Тому **метою статті є** дослідження нового міжнародного та зарубіжного досвіду запобігання порушенням

недоторканності приватного життя з метою урахування кращих його здобутків у вітчизняній превентивній практиці.

Виклад основного матеріалу. Вивчення досвіду запобігання порушенням приватності доцільно проводити на двох рівнях – міжнародному та зарубіжному. Ключову роль на світовій арені відіграють такі міжнародні організації як Організація Об'єднаних Націй (далі – ООН) та Рада Європи (далі – РЄ), а також Європейський Союз (далі – ЄС) як наднаціональне (міжнародне) утворення, а серед зарубіжних країн особливий інтерес становить досвід Федеративної Республіки Німеччина (далі – ФРН), Великої Британії, Японії та Сполучених Штатів Америки (далі – США). Вибір саме цих держав пояснюється тим, що, по-перше, ФРН є країною-членом ЄС та першою державою, де було прийнято нормативно-правовий акт щодо захисту персональних даних; по-друге, Велика Британія – держава, що не так давно вийшла зі складу ЄС шляхом процедури Brexit, і з 2021 р. будує своє законодавство, зокрема й у сфері захисту приватності, не на засадах первинного та вторинного права ЄС, а лише з їх урахуванням; по-третє, Японія та США – провідні країни світу, які не належать до європейської спільноти, однак мають значний вплив на економічні відносини у світі, а також характеризуються специфікою політичних режимів та розбудови законодавства у цілому.

Дослідження досвіду запобігання порушенням недоторканності приватного життя на міжнародному рівні варто розпочати з того, що за даними, які наводить В. Брижко, на сьогодні існує більш ніж 100 міжнародно-правових актів, які прямо або побічно відносяться до правового регулювання захисту персональних даних [18, с. 46]. Усвідомлюючи здобутки та загрози наукового-технічного прогресу у 1968 р. РЄ поставила питання про достатність захисту права на приватне життя, що надають Конвенція про захист прав людини і основоположних свобод (ЄКПЛ) та внутрішнє право держав-учасниць організації. В той же час з подальших досліджень стало відомо про недостатність такого захисту національними законодавствами, тому РЄ прийняла дві важливі резолюції про захист персональних даних, якими встановлено принципи захисту персональних даних у приватному та громадському секторах [21, с. 121]. Важливою для розвитку міжнародного законодавства також є Директива Організації економічного співробітництва та розвитку (ОЕСР) «Про базові принципи захисту недоторканності приватного життя і транскордонних потоків персональних даних» від 23 вересня 1980 р., яка стала першим актом на міжнародній арені, що містить набір базових принципів захисту приватності для обробки персональних даних у транскордонному вимірі. Згодом ці три акти стали основою для розробки ще однієї міжнародної угоди – Конвенції РЄ про захист фізичних осіб при автоматизованій обробці персональних даних ETS № 108 (далі – Конвенція № 108), яка була укладена і відкрита для підписання державами-членами РЄ 28 січня 1981 р.

Конвенція № 108 застосовується до будь-якого процесу обробки даних, що здійснюється у приватному та державному секторах, у тому числі персональних даних судовими і правоохоронними органами, а також їх транскордонної передачі, однак будь-яка держава може застосовувати акт для особистих файлів даних, які не обробляються автоматично, попередньо зробивши відповідну заяву. Принципи Конвенції захищають особу від зловживань, які можуть виникати при збиранні та обробці персональних даних та стосуються, зокрема, відкритого і законного збирання та автоматизованої обробки персональних даних, які зберігаються для визначених і законних цілей, не використову-

ються у спосіб, не сумісний із цими цілями та не зберігаються довше, ніж це необхідно, а також стосуються якості даних, зокрема, передбачають, що такі дані повинні бути адекватними, відповідними, не надмірними (пропорційними) та точними. Акт закріплює за особою право знати про факт збереження про нього/неї інформації і про можливість, за необхідності, її корегування, а обмеження у здійсненні такого права можливі лише за умов існування загрози для інтересів, які переважають (наприклад, інтереси безпеки та захисту держави). Крім того, за відсутності відповідних правових гарантій Конвенцією заборонено здійснювати обробку чутливих даних, які стосуються расової належності, політичних переконань, здоров'я, релігії, статевого життя або засудження в кримінальному порядку, а також накладено деякі обмеження щодо вільного міждержавного обміну персональними даними у тих країнах, які не мають відповідного рівня правового регулювання захисту даних [25, с. 17]. Акт був і залишається єдиним юридично зобов'язуючим міжнародним документом у сфері захисту персональних даних. Крім того, ст. 23 вказує на можливість приєднання держав, які не є членами РЄ, що робить конвенцію не лише «європейською».

У 2018 р. РЄ прийняла Протокол CETS № 223, яким було внесено зміни до Конвенції № 108, таким чином утворилася так звана Конвенція № 108+. У акті використовується нова термінологія, його дія розповсюджується як на автоматизовану, так і на неавтоматизовану обробку, однак не розповсюджується на обробку даних фізичними особами для власних потреб. У Конвенцію № 108+ інтегровано такі принципи, як прозорість, пропорційність, підзвітність, мінімізація даних та конфіденційність за дизайном (privacy by design), а також встановлено додаткові обов'язки держав-учасниць вживати необхідних заходів для дотримання вимог Конвенції № 108+ [30].

Конвенція № 108 заклала підвалини для першої директиви Європейського Союзу про захист даних, прийнятої у 1995 р., яку у 2018 р. замінив GDPR, тому твердження К. Мельник та А. Кардаш про певну спадковість і спорідненість методологічних підходів до захисту персональних даних у праві ЄС та праві РЄ можна вважати цілком обґрунтованими [23, с. 55; 21, с. 123].

Джерелами регулювання сфери персональних даних у ЄС визнаються акти так званого «первинного» та «вторинного» законодавства. Актом первинного законодавства, що регулює аналізовану сферу, виступає Хартія основоположних прав ЄС, яка містить у ст. 8 спеціальну норму, присвячену саме захисту персональних даних. Наявність окремої норми пояснюється розвитком та визначенням цього фундаментального права у висновках і рішеннях Європейської Комісії та Європейського суду [29, с. 57]. Головним актом вторинного законодавства ж на сьогодні є GDPR 2016 р., однак, окрім нього, на території ЄС діє ще ряд директив, які сукупно утворюють так званий «Пакет захисту даних».

GDPR по праву вважають найважливішим стандартом західного світу, який прийнято з метою приведення законодавства ЄС в сфері захисту персональних даних у відповідність до вимог «цифрової ери» та на виконання Стратегії Єдиного Цифрового Ринку Європи. Нові правила застосовуються до обробки даних фізичних осіб у компаніях, підприємствах тощо, які розміщуються не тільки на європейській території, але і здійснюють свою діяльність за межами ЄС і пов'язані з обробкою персональних даних в рамках ЄС, однак не поширюються на: обробку персональних даних для забезпечення національної безпеки і діяльності правоохоронних органів (для цілей попередження, роз-

слідування); обробку персональних даних державами-членами ЄС щодо до загальної зовнішньої політики і політики безпеки ЄС; обробку даних про юридичних осіб; на дані, які відносяться до анонімної інформації і померлих осіб; обробку персональних даних фізичною особою в ході чисто особистої або побутової діяльності і, таким чином, без зв'язку з професійною або комерційною діяльністю [18, с. 49]. Встановлено суворі вимоги до опрацювання персональних даних; обов'язок доведення наявності згоди на опрацювання персональних даних прямо покладається на суб'єкта, що їх збирає; визначено вимоги до privacy policy; введено у дію презумпцію вини порушника тощо. Крім того, GDPR передбачає створення незалежних публічних органів, відповідальних за моніторинг його застосування, що мають слідчі повноваження та право накладати стягнення. Однак, багато положень акту сформульовані абстрактно, а Європейська Комісія не наділена повноваженнями щодо їх конкретизації за допомогою видання правових актів. За кожен випадок витоку персональних даних (незалежно від причин) – 20 млн євро для великих компаній чи до 4% загального глобального річного обігу підприємства за попередній фінансовий рік (залежно від того, яка сума є вищою). Лише за два роки функціонування Регламенту було стягнуто майже 360 млн євро, що доводить його ефективність [22, с. 275–276].

Трохи іншого бачення проблема недоторканності приватного життя зазнала у діяльності ООН. У своїх актах міжнародна організація не визнає захист персональних даних основоположним правом, хоча право на приватне життя є давно визнаним таким правом у міжнародному правовому порядку. У той же час останні 10 років ООН засуджується масове спостереження і наголошується на його можливому впливі на приватне життя, свободу вираження поглядів та функціонування динамічного демократичного суспільства в цілому. Більш пізні резолюції організації закликають підприємства повідомляти користувачів про збір, використання, поширення та збереження персональних даних, а також запроваджувати прозору політику обробки даних [25, с. 23–24].

Варто погодитися з тезою К. Мельник про неможливість ефективного використання міжнародних правових норм у сфері захисту персональних даних без створення національних механізмів із нагляду та захисту прав та законних інтересів фізичних осіб усіма державами світу [24, с. 63]. Це й підтверджує важливість вивчення досвіду останніх.

Нормативно-правові акти про захист персональних даних у європейських країнах почали прийматися у 1970-х рр., які здебільшого й до сьогодні мають типову назву – закони про захист даних. Першим таким законом вважається нормативно-правовий акт, що введений в дію на землі Гессен в Німеччині у 1970 р. [26, с. 16]. Не дивлячись на те, що його положення були націлені на захист цілісності даних про стан державної влади, а не приватних даних, з цим актом пов'язують походження сучасного законодавства в цій сфері – відображення відповідного права у конституціях держав, прийняття ними відповідних законів, а також створення міжнародних актів, про які йшла мова вище. Тому дослідження досвіду запобігання в окремих державах доцільно розпочати саме з ФРН.

Основоположний закон ФРН 1949 р. не містить закріпленого права на захист персональних даних, однак ст. 10 Основного Закону охороняє таємницю комунікацій. У 1977 р. з'явився перший федеральний закон, що захищав персональні дані німців. Нормативно-правовий акт переглянули напочатку 1990-х рр. та адаптували під нові реалії, окресливши головну мети як захист недоторкан-

ності приватного життя при використанні персональних даних, а згодом і у 2017 р. – на реалізацію вимог GDPR, однак у своїй останній редакції передбачає низку більш суворих положень у порівнянні з Загальним регламентом. На сьогодні у кожній з 16 земель прийняли власні закони в цій сфері, а їх виконання регулюється спеціальними комісіями – шістнадцятьма органами захисту даних (Data Protection Authority, далі – DPA) [19] в кожній із земель і Федеральним уповноваженим із захисту даних і свободи інформації. Німецькі DPA активно карають порушників. Одне з таких покарань було накладено DPA землі Баден-Вюртемберг. Порушником є велика державна організація медичного страхування «AOK Baden Wьrttemberg», а накладений штраф склав 1,24 млн євро за недотримання впровадження відповідних технічних та організаційних заходів [13]. За інформацією Державної комісії з питань захисту даних та свободи інформації в Північному Рейні-Вестфалії за 2019–2022 рр. до місцевого DPA надійшло близько 59,4 тис. проваджень [2, с. 10; 8, с. 13; 9, с. 11; 10, с. 15]. Середній рівень адміністративних штрафів сягав від 100 до 3400 євро [6]. Німецьке законодавство передбачає можливість подати цивільний позов проти компаній-порушників, а також притягнути до кримінальної відповідальності фізичних осіб за «небезпечне розповсюдження персональних даних» (§ 126a Кримінального уложення ФРН) [15].

Говорячи про досвід запобігання порушенням недоторканності приватного життя Великої Британії, варто розпочати з того, що країна не має письмової конституції. У 1998 р. парламент схвалив Закон про права людини, який включив ЄКПЛ до національного законодавства і, таким чином, запровадив право на недоторканність приватного життя [1, с. 105]. Перший закон про захист даних у державі було ухвалено 1984 р., який в подальшому зазнавав змін з урахуванням розвитку права ЄС. Велика Британія як член ЄС у 2018 р. оновила своє законодавство до стандартів GDPR, так з'явився Закон про захист даних 2018 р., так званий «DPA 2018», основною метою якого було доповнити GDPR специфічними положеннями відповідно до потреб держави.

31 січня 2020 р. Велика Британія залишила ЄС, а 01 січня 2021 р. закінчився перехідний 11-місячний період, протягом якого на території держави все ще діяло законодавство ЄС. З 2021 р. GDPR стало частиною внутрішнього законодавства Великої Британії відповідно до Закону про Європейський Союз (Відкликання) 2018 і на разі DPA 2018 і GDPR застосовують практично одні і ті самі стандарти для більшої частини обробки даних у Великій Британії, і є достатніми для того щоб створити чіткий і узгоджений режим захисту даних» [16, с. 26]. Це було зроблено з метою формування нового режиму захисту даних, який запрацював у Сполученому Королівстві після Brexit.

За нагляд і дотримання GDPR Великобританії відповідає Офіс уповноваженого з питань інформації, який має широкі розслідувальні, коригувальні, консультативні повноваження, зокрема, проведення консультацій, видання роз'яснень для бізнесу та населення, проведення аналітичної роботи; можливість видавати попередження або догани за невідповідність; наказувати контролеру та процесору надати будь-яку інформацію, необхідну для виконання своїх завдань; проводити розслідування у формі аудиту захисту даних; перевіряти сертифікати, видані відповідно до GDPR Великобританії, щоб повідомити контролера або обробника про ймовірні порушення; отримувати доступ до всіх персональних даних і всієї інформації, необхідної для виконання завдань контролерів або обробників; GDPR Великобританії дає право

Офісу накладати адміністративні штрафи, тимчасові або остаточні обмеження, включаючи заборони на обробку тощо [11].

А. Кардаш з посиланням на О. Радкевича, вказує, що сучасне законодавство Великої Британії характеризується конкретизацією формулювань складів правопорушень щодо розголошення персональних даних та дотримання ряду принципів у діяльності щодо захисту останніх [21, с. 113; 27, с. 148–149]. Зокрема, GDPR Великобританії передбачає адміністративні штрафи в розмірі до 17,5 млн фунтів стерлінгів або 4% річного обороту компанії в усьому світі протягом попереднього фінансового року [11]. Деякі порушення захисту персональних даних можуть бути кваліфіковані як кримінальні делікти, зокрема, в рамках випадків несанкціонованого доступу до комп'ютерних систем або втручання в них. Відповідно до ст. 1 Закону про зловживання комп'ютером 1990 р. за несанкціонований доступ до комп'ютерних матеріалів особа підлягає засудженню у спрощеному порядку до позбавлення волі на строк не більше 6 місяців або до штрафу, що не перевищує 5 ступеня за стандартною шкалою (до 5 тис. фунтів стерлінгів), або до обох видів покарань одночасно [3].

Інтерес для запобігання порушенням недоторканності приватного життя на теренах України становить досвід такої діяльності у Японії. Основний Закон держави, датований 1946 р., містить чотири статті (ст. ст. 11, 13, 21, 35), присвячені питанням охороні персональних даних [28, с. 118]. Законодавство Японії гарантує право на конфіденційність, тобто визнається право на недоторканність приватного життя, право не розголошувати приватну інформацію без поважної на це причини та, як наслідок, право контролювати власні персональні дані, з чого витікає, що треті особи, які мають доступ до приватних даних інших осіб, не повинні порушувати їх особисті права.

Основним законом щодо захисту даних є Закон про захист приватної інформації (Japan's Act on the Protection of Personal Information, далі – APPI), прийнятий у 2003 р. Акт неодноразово переглядався та оновлювався, щоб відобразити зміни суспільства та технологій, крім того існує законодавча вимога щодо його регулярного оновлення раз на три роки, що востаннє відбулося у 2023 р. Японський APPI є дуже подібним до GDPR [12], також ЄС та Японія домовилися визнати свої системи захисту даних, як еквівалентні, що дозволило безпечний обмін даними [20].

За дотриманням Закону про захист приватної інформації стежить Комісія із захисту приватної інформації Японії (PPC), яка була створена після внесення правок до APPI у 2005 р., і є основним радником, дослідником і правозастосувачем щодо захисту даних і конфіденційності в Японії. Серед обов'язків Комісії є розслідувальні, коригувальні, консультативні та каральні повноваження. Відповідно до внесених змін у 2020 р. штрафи були збільшені до максимуму в 1 млн єн для фізичних осіб (близько 7000 євро) або 100 млн єн для підприємств (приблизно 700 тис. євро), хоча штрафи можуть відрізнятися залежно від тяжкості порушення, сфери застосування тощо [12]. Крім того, фізичній особі може загрожувати позбавлення волі на строк до року [4]. Закон не передбачає конкретних цивільних засобів правового захисту, але порушення Закону можуть бути предметом цивільних позовів про грошову та/або моральну шкоду, а також оголошення з вибаченнями як частину деліктних позовів відповідно до Цивільного кодексу Японії [5].

Розглянуті вище країни є представниками так званої «регулюючої» моделі захисту приватності, оскільки існує посадова особа чи уповноважений орган, який забезпечує вико-

нання положень детально розробленого закону про захист персональних даних. Таку модель обрано ЄС під час створення GDPR, однак вона має свої недоліки, зокрема, різність повноважень контролюючого суб'єкта, нестача засобів захисту тощо. Тому деякі країни світової спільноти уникають схвалення загальних принципів захисту персональних даних, надаючи перевагу так званому «секторальному» регулюванню, тобто наявності комплексу законів про захист даних у окремих сферах. За таким принципом збудована система захисту приватності у США.

У США немає єдиного закону про захист персональних даних. Досліджувана сфера регулюється набором із сотень законів, прийнятих як на федеральному рівні, так і на рівні штатів, що призначений для захисту персональних даних жителів США. Федеральні закони передусім стосуються конкретних секторів, таких як фінансові послуги, охорона здоров'я, телекомунікації тощо. Такими прикладами є Закон про захист конфіденційності водіїв, Закон про захист конфіденційності дітей в Інтернеті, Закон про політику кабельного зв'язку, Закон про чесну кредитну звітність, Закон про захист приватності відео, Закон про перенесення та підзвітність медичної інформації тощо. Паралельно з федеральним режимом, акти на рівні штатів захищають широкий спектр прав на конфіденційність окремих мешканців. Захист, передбачений на місцевому рівні, часто суттєво відрізняється від одного штату до іншого, деякі з них є комплексними, тоді як інші охоплюють такі різноманітні сфери, як захист бібліотечних записів до захисту власників будинків від спостереження безпілотників [14].

Відповідно до федерального законодавства США призначення уповноваженого із захисту даних не є обов'язковим, але деякі акти як загальнодержавного, так і місцевого рівнів, вимагають призначення особи або створення органу, які відповідають за дотримання вимог щодо конфіденційності та безпеки персональних даних у певному секторі правовідносин чи на певній місцевості. З цього випливає й різність у підходах до захисту. Оскільки у США немає центрального органу захисту даних, правозастосовчі повноваження регуляторів залежатимуть від конкретного нормативно-правового акту. Деякі закони дозволяють лише федеральний урядовий примус, деякі – федеральний або примус на рівні штатів, а деякі – через приватне право на позов потерпілих споживачів. Чи будуть санкції цивільними та/або кримінальними, залежить від відповідного закону та самого делікту. Штрафи у межах цивільної відповідальності можуть коливатися від 100 до 50 тис. доларів США за порушення (або за запис), з максимальним штрафом у 1,75 млн доларів США на рік за кожне порушення. Водночас кримінальне законодавство США приділяє велику увагу недоторканності приватного життя громадян. Зокрема згідно з §2511 Титулу 18 Зводу законів США карається штрафом у 500 доларів, позбавленням волі до 5 років, або ж обома видами санкцій одночасно перехоплення й розголошення відомостей, переданих телеграфом, усну або електронним засобом [7], спеціально становлено кримінальну відповідальність за порушення конфіденційності електронної пошти та мовної кореспонденції на сервері та інші правопорушення [17, с. 93]. Федеральне законодавство і кримінальні кодекси штатів містять також загальні і спеціальні норми про різного роду зловживання службовим становищем і незаконне поширення та використання персональних даних.

«Секторальна» модель захисту приватних даних, яку використовують у США, також має певні недоліки, головний полягає в тому, що при появі нових технічних засобів виникає потреба в прийнятті нових законів, таким чином не завжди можна

забезпечити надійний захист даних Використання вузькоспеціалізованого законодавства, яке підсилює дію загального закону та деталізує способи захисту певних категорій інформації, є більш практичним та ефективнішим, зокрема й для України. Такий підхід у доктрині має назву «змішаний» [21, с. 130].

Висновки. Проведений аналіз дає підстави стверджувати про існування у міжнародній спільноті потужної системи захисту персональних даних, яка відповідає реаліям сучасності та має здатність до вчасної модернізації у відповідь на нові виклики. Запобігання та протидія порушенням недоторканності приватного життя здебільшого направлені на контроль за діяльністю юридичних осіб – тримачів величезних масивів персональних даних громадян (компаній, організацій, установ, органів влади тощо), а не пересічних громадян. Важливе місце у цій діяльності відведено посадовим особам або уповноваженим органам, які не лише займаються розслідуваннями порушень законодавства та накладенням стягнень, а й ведуть активну науково-дослідну, аналітичну та просвітницьку роботу серед зазначених суб'єктів й населення. Проведене дослідження підтверджує тезу про те, що чим краще нормативно врегульована така діяльність, тим більш захищеною є приватність. Таким чином, основними векторами модернізації української правової дійсності у сфері протидії та запобігання порушенням приватності мають бути: оновлення законодавства щодо захисту персональних даних, в основу якого має бути закладено GDPR; створення уповноваженого органу з контролюючими, каральними, консультативними, просвітницькими повноваженнями; підвищення рівня етичних стандартів та компетентності працівників (soft та hard skills), які мають доступ до персональних даних громадян; розробка дієвих заходів віктимологічного запобігання. Відповідні вектори слугують основою й для нових наукових пошуків.

У статті досліджено міжнародний та зарубіжний досвід запобігання порушенням недоторканності приватного життя крізь призму охорони та захисту права на персональні дані, а також можливості його застосування у вітчизняній превентивній практиці.

Проаналізовано нормативне регулювання вказаної сфери у таких міжнародних організаціях як РЄ та ООН, а також у ЄС як наднаціональному (міжнародному) утворенні. Встановлено, що РЄ та ЄС мають міцне та стійке нормативне підґрунтя у досліджуваній сфері, а на основі їх норм та стандартів (Конвенція № 108 та GDPR) побудовано законодавства провідних країн світу, незалежно від географічної приналежності до європейської спільноти. Аналіз нормативних приписів в межах діяльності ООН дає підстави стверджувати про невизнання організацією захисту персональних даних основоположним правом, хоча право на приватне життя є давно визнаним таким у міжнародному правовому порядку. В той же час останні роки ООН засуджується масове спостереження і наголошується на його можливому впливі на приватне життя.

Серед зарубіжних країн проаналізовано досвід ФРН, Великої Британії, Японії та США. Встановлено, що ФРН, Велика Британія та Японія є представниками регулюючої моделі захисту приватності, оскільки існує посадова особа чи уповноважений орган, який забезпечує виконання положень детально розробленого закону про захист персональних даних. Виявлено, що у США немає єдиного закону про захист персональних даних, тому

досліджувана сфера регулюється набором із сотень законів, прийнятих як на федеральному рівні, так і на рівні штатів. Така модель має назву «секторальна». Авторкою акцентовано увагу на недоліках обидвох моделей.

Зроблено висновок про те, що використання вузькоспеціалізованого законодавства, яке підсилює дію загального закону та деталізує способи захисту певних категорій інформації, тобто «змішаної» моделі, є більш практичним та ефективнішим, зокрема й для України.

Виділено основні вектори модернізації української правової дійсності у сфері протидії та запобігання порушенням недоторканності приватного життя, серед яких приведення законодавства до стандартів GDPR, створення відповідної інституції контролю, підвищення soft та hard skills відповідних посадових та службових осіб, а також дієве віктимологічне запобігання.

Ключові слова: порушення недоторканності приватного життя, запобігання злочинності, персональні дані, приватне життя (privacy), стандарт GDPR.

Poliakh Ye. Possibilities of application of international and foreign experience of preventing privacy violations in domestic preventive practice

The article examines the international and foreign experience of preventing violations of privacy through the prism of protection and protection of the right to personal data, as well as the possibilities of its application in domestic preventive practice.

The normative regulation of the specified sphere in such international organizations as the Council of Europe and the United Nations, as well as in the EU as a supranational (international) entity, is analyzed. It was established that the EC and the EU have a strong and stable regulatory basis in the researched field, and on the basis of their norms and standards (Convention No. 108 and GDPR) the legislation of the leading countries of the world was built, regardless of geographical affiliation to the European community. The analysis of regulations within the scope of UN activity gives reasons to assert that the organization does not recognize the protection of personal data as a fundamental right, although the right to privacy is a long-recognized fundamental right in the international legal order. At the same time, in recent years, the UN has condemned mass surveillance and emphasized its possible impact on private life.

Among foreign countries, the experience of Germany, Great Britain, Japan, and the USA was analyzed. It has been established that Germany, the United Kingdom and Japan are representatives of the regulatory model of privacy protection, as there is an official or an authorized body that ensures the implementation of the provisions of the detailed law on the protection of personal data. It was found that there is no single law on the protection of personal data in the USA, so the research area is regulated by a set of hundreds of laws adopted at both the federal and state levels. Such a model is called «sectoral». The author focuses on the shortcomings of both models.

It was concluded that the use of highly specialized legislation, which strengthens the effect of the general law and details the methods of protection of certain categories of information, that is, the «mixed» model, is more practical and effective, in particular for Ukraine.

The main vectors of the modernization of Ukrainian legal reality in the field of countering and preventing violations of privacy are highlighted, including bringing

legislation to GDPR standards, creating an appropriate control institution, improving the soft and hard skills of relevant officials and officials, as well as effective victimological prevention.

Key words: violation of privacy, crime prevention, personal data, private life (privacy), GDPR standard.

Література

1. Banisar D., Davies S. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, 18 J. Marshall J. Computer & Info. L. 1 (1999). 112 p.

2. Block H. Datenschutzbericht der Landesbeauftragten fьr Datenschutz und Informationsfreiheit Nordrhein-Westfalen: fьr die Zeit vom 1. Januar 2019 bis zum 31. Dezember 2019. 152 s. URL: https://www.ldi.nrw.de/system/files/media/document/file/25-datenschutzbericht-ldi-nrw-2.pdf (Last accessed: 23.01.2024).

3. Computer Misuse Act 1990. URL: https://www.legislation.gov.uk/ukpga/1990/18/enacted?view=plain (Last accessed: 23.01.2024).

4. Coos A. Data Protection in Japan: All You Need to Know about APPI. Endpoint Protector. April 5, 2022. URL: https://www.endpointprotector.com/blog/data-protection-in-japan-appi/ (Last accessed: 23.01.2024).

5. Data Protection Enforcement in Japan. URL: https://www.globalcompliancenews.com/data-privacy/data-protection-enforcement-in-japan/ (Last accessed: 23.01.2024).

6. Eingaben, beschwerden und datenpannen. Landesbeauftragte fьr Datenschutz und Informationsfreiheit Nordrhein-Westfalen. URL: https://www.ldi.nrw.de/zahlen-und-daten (Last accessed: 23.01.2024).

7. Federal Criminal Code and Rules: 18 U.S. Code. § 2511 – Interception and disclosure of wire, oral, or electronic communications prohibited. URL: https://www.law.cornell.edu/uscode/text/18/2511 (Last accessed: 23.01.2024).

8. Gayk B. Bericht der Landesbeauftragten fьr Datenschutz und Informationsfreiheit Nordrhein-Westfalen: fьr die Zeit vom 1. Januar 2020 bis zum 31. Dezember 2020. 262 s. URL: https://www.ldi.nrw.de/system/files/media/document/file/26_-bericht-ldi-nrw-1.pdf (Last accessed: 23.01.2024).

9. Gayk B. Bericht der Landesbeauftragten fьr Datenschutz und Informationsfreiheit Nordrhein-Westfalen: fьr die Zeit vom 1. Januar 2021 bis zum 31. Dezember 2021. 130 s. URL: https://www.ldi.nrw.de/system/files/media/document/file/27_datenschutzbericht_2022_ldi_nrw.pdf (Last accessed: 23.01.2024).

10. Gayk B. Bericht der Landesbeauftragten fьr Datenschutz und Informationsfreiheit Nordrhein-Westfalen: fьr die Zeit vom 1. Januar 2022 bis zum 31. Dezember 2022. 239 s. URL: https://www.ldi.nrw.de/system/files/media/document/file/28_datenschutzbericht_2023_ldi-nrw_1.pdf (Last accessed: 23.01.2024).

11. Hickman T., Devina J. Data Protection Laws and Regulations UK 2023–2024. ICLG. July 20, 2023. URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/united-kingdom (Last accessed: 23.01.2024).

12. Japan Act on the Protection of Personal Information (APPI): An Overview. Usercentrics. Feb 1, 2023. URL: https://usercentrics.com/knowledge-hub/japan-act-on-protection-of-personal-privacy-appi/ (Last accessed: 23.01.2024).

13. LfDI Baden-Wьrttemberg verhдngt BuЯgeld gegen AOK Baden-Wьrttemberg – Wirksamer Datenschutz erfordert regelmдЯige Kontrolle und Anpassung. URL: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/06/PM_Bu%C3%9Fgeld-gegen-AOK.pdf (Last accessed: 23.01.2024).

14. Pittman P., Hafiz A., Hamm A. Data Protection Laws and Regulations USA 2023–2024. ICLG. July 20, 2023. URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (Last accessed: 23.01.2024).

15. Strafgesetzbuch (StGB). URL: https://www.gesetze-im-internet.de/stgb/__126a.html (Last accessed: 23.01.2024).

16. Аналіз законодавства про захист персональних даних України: звіт від 14 вересня 2020 р. 55 с. URL: https://ecpl.com.ua/wp-content/uploads/2020/09/UKR_09142020_CEP_Finalnyy-zvit.pdf (дата звернення 23.01.2024).

17. Бєлєнький В. П. Кіберзлочини за законодавством США. Науковий вісник

Міжнародного гуманітарного університету. Сер.: Юриспруденція. 2015. № 17. Том 2. С. 91–93.

18. Брижко В. М. Сучасні основи захисту персональних даних в європейських правових актах. Інформація і право. № 3 (18). 2016. С. 45–57.

19. Власко С. Захист персональних даних: чий досвід може стати в нагоді Україні. Європейська правда. 16 січня 2018 р. URL: https://www.eurointegration.com.ua/experts/2018/01/16/7076152/ (дата звернення: 23.01.2024).

20. Євросоюз і Японія завершили переговори про взаємний захист персональних даних. Укрінформ. 17 липня 2018 р. URL: https://www.ukrinform.ua/rubric-world/2500176-es-i-aponia-stvorat-najbilsu-u-sviti-sistemu-zahistu-personalnih-danih.html (дата звернення: 23.01.2024).

21. Кардаш А. В. Конституційно-правовий захист інформації про особу (порівняльно-правовий аспект): дис. ... канд. юрид. наук. Харків, 2019. 223 с.

22. Кібербезпека та ризики цифрової трансформації компаній: практичний посібник / Ю. І. Когут. Київ: Консалтингова компанія «СІДКОН», 2022. 372 с.

23. Мельник К. С. Правові механізми захисту персональних даних в Європейському Союзі. Правова інформатика. 2013. № 4 (40). С. 55–61. (с. 55)

24. Мельник К. С. Теоретичні та організаційно-правові засади захисту персональних даних в контексті євроінтеграції України. К.: ТОВ «ПанТот», 2016. 126 с.

25. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2015. 216 с.

26. Право на приватність: conditio sine qua non / Харківська правозахисна група; Худож.-оформлювач О. Герчук. Харків: Фоліо, 2003. 216 с.

27. Радкевич О. П. Забезпечення охорони і захисту персональної інформації у Сполучених Штатах Америки та Великій Британії. Вісник Вищої ради юстиції. 2012. № 1 (9). С. 141–153.

28. Радкевич О. П. Цивільно-правова охорона і захист персональної інформації в мережі Інтернет: дис. ... канд. юрид. наук. Київ, 2014. 243 с.

29. Романюк І. І. Охорона права на персональні дані в Україні (цивільно-правовий аспект): дис. ... канд. юрид. наук. Київ, 2015. 267 с.

30. Тотовицька О. Чи відповідає міжнародним стандартам захист персональних даних в Україні? Портал «ГУРТ». 28 січня 2021 р. URL: https://gurt.org.ua/news/informator/66213/ (дата звернення: 23.01.2024).