

УДК 336.714

Кукіна З.О.\*

## ОСНОВНІ АСПЕКТИ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

*У зв'язку з швидким розвитком інформаційних технологій, активізацією обміну інформацією в мережі Інтернет, з'являються нові виклики в сфері захисту персональних даних. Активізація діяльності в соціальних мережах, з одного боку, та відсутність відповідного правового регулювання такої діяльності, ставлять під загрозу право на недоторканість особистого життя осіб. Вбачається необхідним приділити увагу розробці нового та вдосконаленню існуючого правового поля в сфері захисту персональної інформації як в оффлайні так і в мережі.*

**Ключові слова:** захист персональних даних, право на недоторканість особистого життя, приватність, Інтернет.

*With the rapid development of information technology, and facilitation of exchange of information on the Internet, there are new challenges in the field of personal data protection. The increase of activity of social network, on the one hand, and the absence of legal regulation of such activities, on the other – threaten the right to privacy of persons. It appears necessary to pay attention to the development of new and improvement of the existing legal framework on the protection of personal information offline as well as online.*

**Keywords:** data protection, right to privacy, privacy, Internet.

*В связи с быстрым развитием информационных технологий, активизацией обмена информацией в сети Интернет, появляются новые вызовы в сфере защиты персональных данных. Активизация деятельности в социальных сетях, с одной стороны, и отсутствие соответствующего правового регулирования такой деятельности, с другой, ставят под угрозу право на неприкосновенность личной жизни человека. Кажется необходимым уделить внимание разработке нового и совершенствованию существующего правового поля в сфере защиты персональных данных как в оффлайне, так и в сети.*

**Ключевые слова:** защита персональных данных, право на неприкосновенность личной жизни, конфиденциальность, интернет.

**Постановка проблеми.** Глобалізація і технологічний процес здійснили значний вплив на способи збирання, використання та доступу до інформації. Із розвитком інформаційних технологій останнім часом процес захисту інформації стає все складнішим. Важче запобігти небажаному поширенню інформації та передбачити відповідні випадки небажаного витоку даних. В багатьох випадках, починаючи з відкриття банківського рахунку, закін-

\* кандидат юридичних наук, науковий співробітник кафедри порівняльного і європейського права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка.

чуючи реєстрацією в соціальних мережах, людина поширює важливу особисту інформацію у вигляді імені, адреси, номеру кредитної картки. Під впливом США європейські країни все більше уваги приділяють розробці та вдосконаленню законодавства з питань регулювання захисту особистої інформації.

**Аналіз останніх досліджень і публікацій.** Через те, що тема правового регулювання захисту персональних даних є порівняно новою, кількість наукових розробок є обмеженою. Разом з тим, необхідно виділити наступних дослідників як Р. Андерсон, Ю. Базанов, В. Брижко, А. Баранов, І. Забара, В. Копилов, Р. Калюжний, П. Самараті, Е.А. Степанов, М.Я. Швець, І. Цимбалюк та інші.

**Виділення невирішених раніше частин загальної проблеми.** Виходячи з того, що велика частина обміну інформацією відбувається в Інтернеті, залишається неврегульованими питання захисту персональних саме в мережі, наприклад в соціальних мережах.

**Формулювання цілей статті.** В основі законодавства, що регулює захист персональних даних лежить право на недоторканість особистого життя (право на приватність). Однак, право на приватність має різний обсяг і значення в залежності від юрисдикції. Таким чином, нормативні акти, які регулюють використання та захист персональних даних можуть варіюватися від країни до країни.

Можна виділити три основні підходи до законодавства про захист персональних даних. Європейська система представлена найбільш суворим законодавством, яке регулює збір персональної інформації як урядом так і приватними організаціями. В США використовують біфуркаційний підхід, який передбачає як саморегулювання захисту та збору персональних даних приватним сектором, так і державне регулювання даних, зібраних урядом. Деякі латиноамериканські країни прийняли механізм захисту персональних даних на основі приписів так званого «хабеас дата» (*Habeas Data*) – конституційного принципу ряду держав, що передбачає право громадянина в судовому порядку вимагати доступу до будь-яких документів, які його стосуються, та які зберігаються в архівах та установах, в тому числі спеціальних службах. Принцип хабеас дата є відносно новим і вперше був введений в конституції Бразилії 1988 року [1, с.793].

Визначення поняття «приватність» відрізняється в залежності від держави. Ще в кінці XIX століття майбутній суддя Верховного Суду США Луїс Брандес визначив приватність як право особи «бути залишеною у спокої» («right to be left alone»). Узагальнивши різні підходи та нормативні визначення, приватність можна визначити як комплекс з чотирьох складових: інформаційна, тілесна, комунікаційна і територіальна приватність.

Інформаційна приватність стосується правил збору та обігу персональних даних, таких як інформація фінансових, медичних установ, працедавців. Тілесна – відповідає за захист від втручання в фізичний стан людей, наприклад, медичне обстеження організму людини. Комунікаційна приватність вбирає в себе поняття безпеки та приватності листування, телефонних розмов, електронних повідомлень та інших видів комунікацій. Останній вид – територіальна приватність – відповідає за встановлення обмежень на втручання в особисте середовище особи (дім, робоче місце, громадське оточення) [2, с. 5-29].

Загальна декларація прав людини 1948 року і Міжнародний пакт про громадянські і політичні права 1966 року визначають приватність як право не зазнавати безпідставного втручання в особисте і сімейне життя, безпідставного посягання на недоторканість житла, тайну кореспонденції або на честь і репутацію [3]. Обидва міжнародних документи продовжують роз'яснення цього права, наголошуючи на тому, що «кожна людина має право на захист закону від такого втручання або таких посягань» [4].

Рада Європи також визнає право на недоторканість особистого життя як невід'ємне право людини. В статті 8 Європейська конвенція прот захист прав людини і основопо-

ложних свобод захищає право на приватність таким чином: «Кожна людина має право на повагу до її особистого і сімейного життя, житла і таємниці листування. Держава не може втручатися у здійснення цього права інакше ніж згідно із законом та у випадках, необхідних в демократичному суспільстві в інтересах національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням і злочинам, для захисту здоров'я або моралі чи з метою захисту прав і свобод інших людей» [5].

В Європі під «порушенням даних» («data breach») звичайно розуміють випадки, коли відбувається незаконний доступ, збір та поширення персональних даних. Такі порушення можуть бути наслідком випадкових або навмисних дій, які призводять до викрадення, загублення, або розголошення персональних даних.

В січні 2012 року Європейська комісія запропонувала комплексну реформу європейського законодавства щодо захисту персональних даних, яке було прийнято в 1995 році. Тоді 27 держав-членів ЄС імплементували відповідні норми по-різному, що покликала низку розбіжностей у правозастосовній діяльності. Єдиний закон має на меті усунення таких розбіжностей, усунення значного адміністративного навантаження та зменшення витрат приватного бізнесу на 2,3 млрд. євро на рік. Крім того, реформа підвищить рівень довіри споживачів до онлайн сервісів, спричинивши ріст збільшення робочих місць та посилення інноваційних процесів в Європі.

При розробці реформи Європейська комісія визначила три основні проблеми європейського законодавства в сфері захисту персональних даних. Першою проблемою є труднощі, які виникають у фізичних осіб щодо контролю обігу особистої інформації. З огляду на недостатній рівень гармонізації національних законів про захист персональних даних, особам складніше користуватися своїм правом на захист в одних країнах порівняно з іншими, особливо в мережевому просторі. Особи втратили контроль над обігом персональної інформації через великий обсяг даних, які розповсюджуються в мережі без їхнього відома. Крім того, розповсюдженою є думка, що поширення персональних даних є частиною сучасного життя і 72% європейських користувачів Інтернету вважають, що від них вимагають забагато особистої інформації. Часто вони навіть не знають, яким чином використовувати свої права в Інтернеті.

Другою проблемою є прогалини та невідповідність в правовому регулюванні захисту персональних даних в сфері судового співробітництва в кримінальних справах. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», виключає судове співробітництво в кримінальних справах з предмету регулювання [6]. Постанова Ради Європейського Союзу № 2008/977/ЖНА від 27.11.2008 року «Про захист персональних даних в рамках поліцейського та судового співробітництва у кримінальних справах» відображає особливості до-лісабонської (опорної) структури ЄС та характеризується обмеженим колом питань та наявністю прогалин в сфері, які викликають невпевненість громадян та органів влади в питання застосування відповідного законодавства, а також практичні труднощі з приводу його імплементації [7]. Крім того, постанова дозволяє відступати від загальних принципів захисту персональних даних на національному рівні. Таке регулювання не тільки шкідливо впливає на процес гармонізації, але перешкоджає вільному обміну персональними даними між державами-членами.

Третьою проблемою є бар'єри для бізнесу та органів державної влади в результаті фрагментації, правової невизначеності і непослідовним застосування законодавства про захист персональних даних. Незважаючи на мету Директиви 95/46/ЄС забезпечувати однаковий рівень захисту інформації в ЄС, в окремих країнах існує суттєва різниця в пра-

вовому регулюванні такого захисту, нерівномірність в повноваженнях та ресурсах відповідальних за цю сферу державних органів. Внаслідок цього, утворюється фрагментарне законодавче середовище, яке спричинює нерівномірний захист громадян ЄС. Така нерівність також призводить до непотрібних адміністративних витрат та створює значний фінансовий тягар для компаній, які здійснюють транскордонні операції.

Таким чином, оголошена реформа в сфері захисту персональних даних покликана вирішити три наявні проблеми через гармонізацію відповідного законодавства в державах-членах [8].

В більшості країн право на приватність користується конституційним захистом. В США та Канаді, наприклад, право на приватність формулюється в численних положеннях проти необґрунтованих обшуків та арештів. Верховний суд США зазначав, що Конституція захищає «особистий інтерес уникаючи розкриття інформації щодо особистих справ людини» та «інтерес до самостійності в прийнятті певних важливих рішень». При розробці концепції приватності за основу визначення Верховний суд використав IV поправку конституції. Вона забороняє довільні обшуки і арешти, а також вимагає, щоб ордери на арешт мали підставу і були санкціоновані судом.

В країнах Латинської Америки конституційне визначення приватності зводиться до права не зазнавати безпідставного втручання в особисте життя людини, сім'ю, житло, таємницю кореспонденції, і право бути вільним від нападів на честь людини і її репутацію. Таке визначення відповідає дефініціям Загальної декларації прав людини і Міжнародного пакту про громадянські і політичні людини. Деякі конституції включають в себе право на захист даних і положення про хабеас дата.

Значний внесок в розробку керівних принципів, рекомендацій, а також імперативних правових норм в сфері захисту персональної інформації зробили міжнародні організації, серед яких потрібно відмітити Організацію економічного співробітництва та розвитку (ОЕСР), Азійсько-Тихоокеанське економічне співробітництво (АТЕС) та ін. Якщо узагальнювати правотворчу практику цих організацій в сфері регулювання захисту особистої інформації, то можна сформулювати певні універсальні принципи за якими персональна інформація повинна:

1. бути отримана на законних підставах;
2. бути використана таким чином, який сумісний з першочерговою зазначеною метою;
3. бути точною, актуальною та пропорційною по відношенню до мети;
4. містити точну та актуальну інформацію;
5. мати обмежений доступ з боку третіх осіб;
6. бути знищена після досягнення поставленої мети.

В той же час різні країни мають деякі суттєві відмінності в підходах, представлених в документах зазначених організацій. Такі відмінності стосуються того, коли і як застосовувати зазначені принципи щодо державних органів, приватних комерційних підприємств, і навіть фізичних осіб, а також питань кримінального права та національної безпеки [9].

В Україні в 2010 році був прийнятий закон «Про захист персональних даних», який є основним документом, який регулює обіг персональних даних. 23 липня 2013 року Президент України підписав Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», № 383-VII, який вступить в силу з 1 січня 2014 року [10].

Законом вводиться певні зміни та додаються уточнення до Закону України «Про захист персональних даних», ратифікаційного закону Конвенції про захист осіб у зв'язку з

автоматизованою обробкою персональних даних 1981 року та Кодексу про адміністративні правопорушення.

Нововведеннями є вилучення із переліку суб'єктів уповноваженого державного органу з питань захисту персональних даних Державної служби захисту персональних даних і передача її функцій контролю до Уповноваженого Верховної Ради України з прав людини. Крім того, ліквідується система реєстрації баз персональних даних, яка заміняється повідомленням Омбудсмена про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних.

Органи державної влади та органи місцевого самоврядування, а також володільці баз даних мають визначати відповідальний підрозділ (особу), що організовує роботу, пов'язану із захистом персональних даних при їх обробці. Інформацію про зазначений структурний підрозділ (особу) необхідно повідомляти Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення.

За законом володільць персональних даних визначається (по-новому), як фізична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Закон вносить зміни в перелік прав суб'єкта персональних даних і пов'язаних з ними обов'язків володільця. Так, при зміні мети обробки персональних даних на нову, що є несутісною з попередньою згода суб'єкта є необхідною. Розширений перелік чутливих даних – додано біометричні і генетичні. Водночас з переліку вилучено звинувачення у злочині.

За оновленим законом суб'єкт матиме право, зокрема:

- знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних, а також отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;
- звертатися із скаргами на обробку своїх персональних даних до Уповноважений або до суду;
- Закон змінює зміст функцій Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних.

Згідно вищевказаного Закону Омбудсмен матиме:

- право на перевірки, як за скаргами так і за власною ініціативою;
- доступ до будь-якої інформації (документів) (у т.ч. з обмеженим доступом) володільців або розпорядників персональних даних, які необхідні для здійснення контролю відповідних баз даних чи картотек, інформації з обмеженим доступом;
- право затверджувати нормативно-правові акти у сфері захисту персональних даних, за підсумками перевірки, розгляду звернення;
- право видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень;
- право надавати рекомендації щодо практичного застосування законодавства, роз'яснювати права і обов'язки відповідних осіб;
- право складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду і т.д.

З 1 січня 2014 року зміниться характер винятків із закону. Обробка даних буде можлива без застосування положень закону фізичною особою виключно для особистих чи по-

бутових потреб, а також виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів. Таким чином зникає законодавча прив'язка до професії журналіста. Крім того, в законі зазначено, що дію статей що регулюють загальні питання обробки персональних даних, чутливих персональних даних та прав суб'єктів може бути обмежено в цілях захисту інтересів національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

Остання зміна стосується статті 188 Кодексу України про адміністративні правопорушення, яка встановлює санкції за порушення зобов'язань щодо повідомлення та реагування на приписи Омбудсмана, порушення порядку обробки персональних даних.

Такі зміни є позитивними, але в той же час вони не перекривають усі недоліки українського законодавства в сфері захисту персональних даних. Так в законопроекті «забули» визначити згоди суб'єкта персональних даних. Крім того, в вересні був зареєстрований законопроект, який вносить зміни до Закону України «Про доступ до публічної інформації», який пропонує визнати конфіденційною будь-яку інформацію про фізичних осіб та обмежити та оприлюднювати її лише з дозволу цих самих осіб. Підставою для такого обмеження є захист персональних даних. Але така підстава є перебільшенням, адже занадто високий рівень захисту може призвести до обмеження поширення інформації, яка має важливий суспільний інтерес.

**Висновки.** Останнім часом уряди держав і міжнародні організації все більше уваги приділяють захисту персональних даних індивідів. Основним приводом для підвищення уваги став швидкий розвиток технологій та відсутність достатньо ефективної регламентації інформаційних відносин в мережі Інтернет. Реформа Європейського союзу, гармонізація законів держав-членів, зміни в законі «Про захист персональних даних» в нашій країні свідчать про проведення активних дій в напрямку вдосконалення відповідного нормативного регулювання захисту права особи на приватне життя, як фундаментального права людини.

#### Список використаних джерел

1. Большой юридический словарь / под ред. А. Я. Сухарева – 3-е изд. – М.: ИНФРА-М, 2006. – С. 793.
2. «Приватність і права людини». Звіт Privacy International – В кн.: «Свобода інформації та право на приватність в Україні», т.2. – Харків : Фоліо, 2004, с. 5-29.
3. Загальна декларація прав людини. — К. : Укр. Правнича Фундація. – Вид-во Право, 1995. — 12 с.
4. Міжнародний пакт про громадянські і політичні права (1966) // Права людини і професійні стандарти для юристів в документах міжнародних організацій. – Амстердам; К., 1996.
5. Preliminary Comments on a Statement of Principles for Privacy and Personal Data Protection in the Americas, [Electronic resource]. – Access mode: CJI/doc.382/11. <http://www.oas.org/en/sla/iajc/docs/INFOANUAL.CJI.2011.ENG.pdf>.
6. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних». [Електронний ресурс] – Режим доступу: [http://zakon4.rada.gov.ua/laws/show/994\\_242](http://zakon4.rada.gov.ua/laws/show/994_242).
7. Постанова Ради Європейського Союзу № 2008/977/ЖНА від 27.11.2008 року «Про захист персональних даних в рамках поліцейського та судового співробітництва у кримінальних справах» [Електронний ресурс] – Режим доступу: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF>.

8. Commission Proposals on the data protection reform: legislative texts Commission staff working paper. Impact assessment. Brussels, 25.1.2012 SEC (2012) 72final [Electronic resource]. – Access mode: [http://ec.europa.eu/justice/data-protection/document/review2012/sec\\_2012\\_72\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf).
9. Comparative Study: Data protection an the Americas. Permanent Council of Organization of American States. OEA/Ser. CP/CAJP-3063/12, 2012.
10. Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» від 03.07.2013 р. № 383–7. – Офіційний вісник України, 2013. – № 57. – С. 25.