

МІЖНАРОДНИЙ ДОСВІД ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ

У статті здійснюється аналіз міжнародного досвіду з питань правового регулювання захисту персональних даних у мережі Інтернет. Як основні регулюючі документи розглядаються Конвенція № 108 та Керівні принципи ОЕСР. Визначається різниця в підходах різних національних законодавств та основні орієнтири у процесі національного регулювання захисту персональних даних у цій сфері.

Ключові слова: персональні дані; захист персональних даних; база персональних даних; міжнародна гарантія захисту.

Кравчук М. Н. Международный опыт правового регулирования защиты персональных данных в сети Интернет.

В статье проводится анализ международного опыта по вопросам правового регулирования защиты персональных данных в сети Интернет. В качестве основных регулирующих документов рассматриваются Конвенция № 108 и Руководящие принципы ОЭСР. Определяется разница в подходах разных национальных законодательств и основные ориентиры в процессе национального регулирования защиты персональных данных в этой сфере.

Ключевые слова: персональные данные; защита персональных данных; база персональных данных; международная гарантия защиты.

Kravchuk M. M. International Experience of Legal Regulation of Personal Data Protection in the Internet.

This article analyzes the international experience in the legal regulation of personal data protection on the Internet. The Convention № 108 and OECD Guidelines as the main regulatory documents are examined in this article. The difference in the approaches of different national legislations and the major landmarks in the area of national regulation of personal data protection in this area are determined.

Keywords: personal data; personal data protection; personal data base; international protection warranty.

Законодавство європейських країн у сфері захисту персональних даних починає формуватися з 80-х рр. минулого століття. Зокрема, у 1983 році Федеральний Конституційний суд ФРН вказав на необхідність розробки законодавчих актів стосовно захисту індивідуальної інформації у зв'язку з правом користувача знати інформацію про себе, а також про те, яким чином його персональні дані використовуються та розкриваються. Результатом семирічної роботи стало прийняття у 1990 році Закону ФРН «Про захист даних» [4; 7]. Незважаючи на те, що цей закон був прийнятий у цій країні пізніше, ніж у деяких інших європейських державах, він вважається найбільш досконалим у порівнянні з подібними законодавчими актами інших країн.

Серед інших європейських країн варто назвати: Фінляндію (Закон «Про реєстрацію громадян» 1987 року), Нідерланди (Декрет про вразливі дані 1993 року), Великобританію («Закон про захист персональних даних» 1984 року), Францію (Закон «Про інформатику, картотеку та свободи» 1978 року), Угорщину (Закон «Про захист інформації про особу і доступ до інформації, що становить суспільний інтерес» від 1992 року). Серед країн Азії перед веде Гонконг, який у 1995 році прийняв закон про захист персональних даних і на його основі закони «Про практику стосовно номерів посвідчення особи» та «Про дані стосовно кредитоспроможності споживачів» [4; 7].

Провідну роль у сфері міжнародного захисту персональних даних відіграє європейська спільнота. Ще 28 січня 1981 року Радою Європи була прийнята так звана Конвенція № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [2]. Ця Конвенція стала першою спробою створення єдиного міжнародного законодавчого акта, який би ставив за мету захист персональних даних. Цей документ спрямований на об'єднання країн світу для визначення основних вимог до передачі індивідуальної інформації про людину у всесвітньому електронному просторі, тобто створення низки правил, які стають обов'язковими при обробці персональних даних. Першими країнами, які приєдналися до Конвенції № 108, були Франція, Швеція,

Німеччина, Іспанія та Норвегія. Вже у 2000 році рішення про приєднання прийняли більше двадцяти країн. У преамбулі до Конвенції № 108, зокрема, зазначається: «держави – члени Ради Європи, які підписали цю Конвенцію, враховуючи, що метою Ради Європи є досягнення більшого єднання між її членами, зокрема на основі поважання верховенства права, а також прав і основних свобод людини, зважаючи на доцільність поширення гарантій прав і основних свобод кожної людини, і зокрема права на повагу до особистого життя з огляду на зростання транскордонного потоку даних особистого характеру, які піддаються автоматизованій обробці, підтверджуючи в той же час свою відданість свободі інформації незалежно від кордонів, визнаючи необхідність узгодження основоположних цінностей поваги до особистого життя та безперешкодного обміну інформацією між народами, погодилися [...] підписати цю Конвенцію» [2]. Отже, ця Конвенція стала своєрідною «квінтесенцією» досвіду європейських країн у захисті персональних даних та їх обробці.

Причиною для більш глибокого вивчення проблеми захисту персональних даних в європейській спільноті стали дві резонансні справи. Перша з них – це ситуація довкола заборони французьким агентством із захисту персональних даних передачі інформації, що стосувалася французьких працівників відомого автомобільного концерну, до головного офісу концерну в Італії. Причина полягала в тому, що зазначений концерн не міг гарантувати достатній рівень захисту персональних даних та не погодився із законодавством Франції у цій сфері. Другий випадок пов'язаний з відмовою німецького банку передати інформацію про своїх клієнтів, які були громадянами Німеччини, до свого офісу, що знаходився в Гонконгу [3].

15 грудня 1997 року Європейський Парламент прийняв Директиву 97/66/ЄС «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» [1]. Ця Директива встановлює вимоги для впровадження у національне законодавство гарантій щодо захисту персональних даних. З цією метою при Раді Європи утворюється особливий орган, так звана «Робоча група 29-ої статті». Задача його полягає в нагляді за державами, що увійшли до Конвенції № 108, та дотримання ними вимог Директиви 97/66/ЄС у захисті персональних даних при обробці інформації в автоматизованих базах даних. З часом з метою адаптування попереднього законодавства у цій сфері до змін на ринку та у технологіях надання послуг електронного зв'язку її замінила Директива № 2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних та захисту права на недоторканість особистого життя в сфері електронних засобів зв'язку (Директива про право на недоторканість особистого життя та електронні засоби зв'язку) [1], прийнята 12 липня 2002 року, яка мала забезпечити уніфікований рівень захисту персональних даних та інформації про приватне життя користувачів загальнодоступних послуг електронного зв'язку незалежно від технологій, що використовуються.

Іншими документами, завданням яких є посилення вимог до захисту персональних даних, стали Директива 2002/20/ЄС Європейського Парламенту і Ради від 7 березня 2002 року про дозвіл для мереж і послуг електронних засобів зв'язку (Директива про дозвіл), Директива 2002/22/ЄС Європейського Парламенту і Ради від 7 березня 2002 року про універсальну послугу і права користувачів стосовно мереж і послуг електронного зв'язку (Директива про універсальну послугу) та Директива 2009/136/ЄС Європейського Парламенту і Ради від 25 листопада 2009 року, що вносила зміни до ряду раніше ухвалених документів, які регулюють діяльність у цій сфері [9]. Для європейської спільноти вони стають основними інструментами для захисту персональних даних. Однією з цілей зазначених правових інструментів є майбутнє створення європейської зони вільного руху інформації У свою чергу Україна, у світлі своїх євроінтеграційних сподівань, ухвалила 1 червня 2010 року Закон України «Про захист персональних даних» [8].

Перерахуємо принципи, на яких базуються директиви Європейського Союзу, що є базовими для захисту персональних даних:

– персонорентризм (автоматизовані системи обробки персональних даних створені для обслуговування потреб людини). Тобто, людина є самоціллю для будь якої діяльності держави. Держава та інші формування, в першу чергу, повинні слугувати людині та не ставити під сумнів цінність її свободи;

– екстериторіальність (незалежно від місцезнаходження баз обробки персональних даних та місцезнаходження фізичних осіб, особисті дані яких зберігаються та оброблюються, мають базуватися на повазі до основних прав та свобод людини). Обмеження за територіальними ознаками неприпустимі в сфері захисту персональних даних. Цей принцип походить з основних положень Загальної декларації прав людини ООН від 10 грудня 1948 року [6];

- зв'язок юридичних прав на захист персональних даних та невтручання в особисте життя людини;
- рівність захисту персональних даних у всіх країнах-членах та невчинення перешкод на шляху передачі таких даних. Що означає: країни – учасники Конвенції гарантують належний захист індивідуальної інформації, всі майбутні країни-члени, які побажають приєднатися до цієї Конвенції, повинні надати гарантії виконання основних прописаних у ній вимог;
- субсидіарність (будь-яка обробка індивідуальної інформації про фізичну особу повинна відбуватися на основі законодавства країни-члена, повноважень створеного нею контролера, рівень можливих ризиків втрати або витоку інформації базуються на національних законодавчих базах);
- зближення законодавств в сфері захисту персональних даних не повинно бути причиною зниження рівня безпеки, а навпаки – служити підвищенню якості послуг захисту персональної інформації. Довіра до нової держави – члена Конвенції та Директиви повинна ґрунтуватися на конкретних кроках держави-члена до надання гарантій захисту персональних даних. В іншому випадку прийняття такої держави стає неможливим через зниження загального рівня захисту при її вступі до Конвенції;
- принципи захисту персональних даних повинні бути однаковими як для автоматизованих баз, так і для інших форм ведення баз даних;
- збір та обробка персональних даних повинні проводитися на основі чітко визначених та законних цілей;
- дозвіл використання персональних даних у разі захисту життєво важливих для суб'єкта інтересів;
- дозвіл на використання персональних даних у разі виправдання їх обробки суспільними цілями в сфері охорони здоров'я, соціального захисту, в науковій сфері та в державних статистичних дослідженнях;
- держави-члени можуть у своєму законодавстві встановлювати спеціалізацію за сферами для отримання індивідуальної інформації. Медична інформація видається медичним працівником, інформація соціального захисту – соціальним агентом тощо;
- контрольний орган держави-члена може наділятися правами з метою захисту інтересів національної безпеки, забезпечення основних прав громадян, захисту економічних та фінансових інтересів держави.

Кожна з держав – членів Конвенції № 108 бере на себе зобов'язання приводити своє законодавство у сфері захисту персональних даних у відповідність до викладених вище принципів [2]. Для України виконання цих вимог є однією з обов'язкових умов на шляху до євроінтеграції.

Крім європейського досвіду у сфері захисту персональних даних, слід звернути увагу і на специфіку вирішення цієї проблеми в США. Точкою відліку постановки проблеми захисту індивідуальної інформації в США став випадок у Бостоні у 1890 році, коли на шпальтах однієї з газет були опубліковані деякі подробиці одного весілля. Процес проти газети почав батько нареченої, відомий в той час адвокат та юрист Самуель Воррен. У результаті у зазначеній статті, присвяченій захисту інформації особистого характеру, вперше визначається поняття «захист персональних даних» як синонім «бути залишеним у спокої» [5]. Саме подальший розвиток цієї концепції і призвів до появи у Загальній Декларації прав людини ООН від 10 грудня 1948 року статті 12: «Ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь та гідність. Кожна людина має право на захист закону від такого втручання або посягань» [6].

Щодо американської специфіки захисту персональних даних передусім слід зазначити, що законодавство США є досить жорстким та й надалі тільки посилює відповідальність за втрату або незаконний доступ до баз персональних даних. Наразі до Конгресу США внесений черговий законопроект, згідно з яким посилюється захист суб'єктів, персональні дані яких обробляються, від незаконних втручань та втрати їхніх даних у мережі Інтернет. Якщо такий закон буде прийнято, то за порушення у сфері захисту індивідуальної інформації злочинцям загрожує штраф до 1 млн. доларів США або ув'язнення до 5 років. За новим законодавством США заборонена інсталяція програмного забезпечення для збору індивідуальної інформації, ідентифікації користувача, без його відома та згоди. Передбачена також відповідальність за підтасування результатів пошукової видачі з метою заманювання на комерційні сайти, подробиці сторінки і рекламу, і при цьому «чорні оптимізатори», які займаються подібною діяльністю, отримують

винагороду в грошових та інших еквівалентах. Організації, клієнтська база яких перевищує 10 тис. записів, зобов'язані дотримуватися загальних правил, визначених американським законодавством. Це робиться з метою захисту інформації від витоку і безпідставного знищення. Ухилення від виконання вимог загрожує суворими санкціями та штрафами. Загалом, за підрахунками незалежних статистичних компаній та авторів законопроекту, загальний збиток, завданий громадянам США та самій державі внаслідок таких дій, майже досяг відмітки у 10 млн. доларів.

Діяльність в інтернет-просторі США регламентується набагато жорсткіше, ніж у Європі. До того ж, у Сполучених Штатах визначена кримінальна відповідальність за неналежне зберігання та обробку персональної інформації та її знищення не за законом, на відміну від Європейського Союзу, де кримінальні справи можуть заводитися тільки у разі завдання шкоди державній безпеці та основним правам громадян. Для європейських держав неналежне поводження з персональними даними віднесено до адміністративних правопорушень, і в Україні, зокрема, карається значними штрафами (від двохсот до трьохсот неоподаткованих мінімумів).

Досвід європейських країн та США в сфері захисту даних сприяв початку дослідження цієї проблеми Організацією Економічної Співпраці та Розвитку (ОЕСР), яка розпочала активну діяльність у цьому напрямку у 1969 році. Саме тоді виникають спроби вивчення комп'ютеризації та автоматизації обробки даних. У 1978 році ОЕСР створює групу експертів, основною спеціалізацією якої стають випадки транскордонної передачі інформації та захист відповідних даних. Керівником цієї групи стає представник Австралійського Комітету з правової реформи [5].

23 вересня 1980 року ОЕСР ухвалила Керівні принципи про захист права на приватність та транскордонні потоки інформації [3]. Ці принципи не покладають на держав-членів особливих зобов'язань, але обмежують деякі виключення з установлених ними правил. До того ж Керівні принципи поширюються не тільки на автоматизовані бази даних, а й на «змішані» системи, в яких методи обробки здійснюються не за допомогою комп'ютерних засобів.

У 1998 році в Канаді на засіданні ОЕСР, на якому були присутні представники 29 країн-членів, була прийнята Декларація про захист інформації в глобальних мережах, у тому числі й мережі Інтернет. Для Декларації важливим аспектом є попередження користувача мереж про можливі проблеми приватності, навчання користувачів основним правилам захисту персональних даних, їх правам та обов'язкам [6].

Отже, роблячи попередні висновки, стає можливим визначити основні орієнтири в сфері національної регуляції захисту персональних даних та міжнародний досвід у вирішенні цієї проблеми. Зусилля держав – членів Конвенції № 108 [3] та ОЕСР сприяли приведення законодавств багатьох країн до стандартизації захисту прав споживачів щодо захисту та обробки персональних даних не тільки в мережі Інтернет, а й взагалі в усіх мережевих системах. Виконання вимог Директиви 97/66/ЄС значно підвищило рівень безпеки при транскордонних потоках передачі персональних даних та їх надійного збереження в країнах, що взяли на себе відповідальність за виконання вказівок Директиви. При цьому різниця в підходах національних законодавств нівелюється досягненням основної мети – забезпечення основних прав людини.

Список використаних джерел:

1. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15 грудня 1997 року [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/994_243; Директива № 2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних та захисту права на недоторканість особистого життя в сфері електронних комунікацій (Директива про право на недоторканість особистого життя та електронні засоби зв'язку) від 12 липня 2002 року [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/rada/show/994_b34.
2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р. [Електронний ресурс]. — Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_326.
3. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації : дис. ... канд. юрид. наук / А. В. Пазюк . – К., 2004 р. – 205 с.
4. Попов А. О. Зарубіжний досвід правового регулювання захисту відомчих інформаційних ресурсів / А. О. Попов // Форум права. – 2009. – № 3. – С. 513–519.
5. Пазюк А. В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти [Електронний ресурс] / А. В. Пазюк // МГО Прайвесі Юкрейн. – К. : Інтертехнодрук,

2000 р. – Режим доступу :
<https://docs.google.com/document/d/1hvVJPeoCVqBAauBZWjopyn58h1VbBehAucIDV0uYEU/edit?hl=ru&pli=1>.

6. Загальна Декларація прав людини ООН від 10 грудня 1948 року [Електронний ресурс]. – Режим доступу :
http://zakon2.rada.gov.ua/laws/show/995_015?test=XX7MfyrCSgkyS5FIZiTWTZNHdlyUsFggkRbI1c.

7. Інформаційне законодавство : Збірник законодавчих актів: У 6 т./ За заг. ред. Ю. С. Шемшученка, І. С. Чижа. – Т. 5. Міжнародно-правові акти в інформаційній сфері. – К. : ТОВ «Видавництво «Юридична думка», 2005. – 328 с.

8. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI [Електронний ресурс]. – Режим доступу : <http://zakon4.rada.gov.ua/laws/show/2297-17/page>.

9. Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) [Електронний ресурс]. – Режим доступу : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0021:0021:EN:PDF>; Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) [Електронний ресурс]. – Режим доступу : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0051:EN:PDF>; Directive 2009/136/ec of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [Електронний ресурс]. – Режим доступу : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF>.

** Кравчук Марія Миколаївна – помічник-консультант народного депутата України.*