УДК 341.24

Авраменко А.В.
прокурор відділу прокуратури м. Києва

ПЕРЕДОВИЙ МІЖНАРОДНИЙ ДОСВІД ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ

Постановка проблеми. Розбудова в Україні демократичної, соціальної, правової держави, найвищою цінністю в якій визнаються людина, її життя і здоров'я, честь і гідність, недоторканність і безпека та підтримання ефективного функціонування державних інститутів, пов'язана з необхідністю вдосконалення захисту суб'єктивних громадянських прав. Починаючи з 80-х рр. XX ст. у США та країнах Європи серед таких прав стали виокремлюватися права на приватність та недоторканність інформації про особу. Нещодавно до числа країн, що піклуються про непоширення персональних даних про особу, в тому числі працівника, приєдналася і Україна. Однак розвиток відповідного законодавства відбувається переважно шляхом запозичення іноземного досвіду правового регулювання цих суспільних відносин. Тому доцільно комплексно поглянути на передовий міжнародний досвід у цій сфері.

Актуальність теми дослідження підтверджується недостатністю кількості наукових робіт, заснованих на новітніх концепціях та міжнародному досвіді, присвячених тематиці захисту персональних даних працівників та удосконаленню нормативно-правової бази у цій сфері.

Огляд останніх досліджень і публікацій. У національній правовій школі питанням вивчення міжнародного досвіду правового регулювання забезпечення прав працівників присвячено чимало наукових робіт. Деякі аспекти означеної проблематики зачіпали у своїх працях такі науковці, як В.М. Брижко, С.В. Венедіктов, Ю.І. Крилова, М.В. Різак, І.М. Сопілко, В.І. Теремецький, Д.М. Цвірюк, Р.І. Чанишев, А.М. Чернобай та ін. Водночас у наукових працях передовий міжнародний досвід захисту персональних даних працівника розглядається фрагментарно, а комплексні дослідження у цій сфері майже відсутні.

Формулювання завдання дослідження. Метою статті є дослідження передового міжнародного досвіду захисту персональних даних працівника.

Виклад основного матеріалу. Особливе значення в розробці пропозицій, спрямованих на удосконалення національного законодавства в досліджуваній сфері, має досвід деяких зарубіжних країн, законодавство яких містить норми, що чітко закріплюють поняття персональних даних, визначають дієвий механізм їх захисту.

Так, одним із показових прикладів функціонування ефективного механізму захисту персональних даних, у тому числі у сфері трудової діяльності, є США. У цій країні діють одні з найбільш жорстких умов використання персональних даних, які прирівнюються до групи конституційних прав, що забезпечують недоторканність особи та її приватного життя.

До системи законодавства США у сфері захисту персональних даних належать закони «Про захист конфіденційності відеоматеріалів» (The Video Privacy Protection Act) 1980 р., «Про захист користувачів кабельних мереж» (The Cable Television Consumer Protection and Competition Act) 1992 р. Аналізуючи зазначені закони, деякі науковці цілком справедливо стверджують, що в умовах інформатизації ці акти відіграють важливу роль у гарантуванні прав людини та громадянина на захист персональних даних і особисту недоторканність. Крім того, наголошується, що у США діє концепція захисту інформації незалежно від

носія такої інформації, а, отже, її захист здійснюється на загальних підставах (як і матеріальних цінностей) [1, с. 58–59].

В.І. Теремецький та Д.М. Цвірюк зазначають, що політика США у сфері захисту персональних даних має комплексний характер, оскільки в державі прийнято значну кількість нормативно-правових актів, які регламентують питання захисту інформації персонального характеру в окремих сферах суспільного життя. Як приклад науковці наводять закон «Про право на фінансову приватність» (The Rightto Financial Privacy Act) 1978 р. Йдеться про встановлення заборони надання інформації персонального характеру державним установам за винятком випадків, коли відомості потрібні для проведення судового або адміністративного розслідування чи реалізації іншої законної діяльності [2, с. 75].

Як відомо, США є країною з високим рівнем запровадження в усі сфери суспільного життя інформаційно-телекомунікаційних технологій, тому не дивує той факт, що захисту персональних даних у мережі Інтернет та інших системах у державі приділяється багато уваги.

З цього приводу М.М. Кравчук зазначає, що діяльність в інтернет-просторі США регламентується набагато жорсткіше, ніж в Європі. Проводячи порівняльний аналіз законодавства у сфері захисту персональних даних у США та країнах Європи, вчена вказує, що 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. В європейських державах неналежне поводження з персональними даними зараховане до адміністративних правопорушень, а в Україні, зокрема, карається значними штрафами (від двохсот до трьохсот неоподаткованих мінімумів) [3, с. 124].

Наведені вище гарантії повною мірою поширюються на правовідносини, що виникають у сфері захисту персональних даних працівника. Разом із тим у США питання щодо збору та обробки роботодавцем персональних даних про працівника (потенційного працівника) більш детально регламентовано.

Зокрема, загальноприйнятою у цій державі є практика проведення детального розслідування особистого життя працівника, яке проводиться роботодавцем до укладення трудового договору та виражається у проведенні медичних аналізів на наркотики та алкоголь, дослідженні особистої справи водія, дослідженні професійного стажу та наявності судимості. Крім того, для процедури працевлаштування характерною є перевірка кредитної історії працівника, яка здійснюється на підставі закону про добросовісність у наданні відомостей про кредитоспроможність. Іншим федеральним законом у сфері збору інформації про працівника є закон про захист працівника від застосування поліграфу, який забороняє більшості приватних роботодавців застосовувати детектор. Водночас відповідно до закону про захист електронних систем зв'язку електронні листи працівника є власністю роботодавця, якщо вони направляються із комп'ютерної системи останнього. Також цей закон дає змогу встановлювати роботодавцю камери спостереження, крім місць приватного користування [4, с. 132].

Таким чином, інститут захисту персональних даних працівника в США характеризується такими особливостями:

1) законодавством встановлюються досить жорсткі правила та вимоги до обробки персональних даних, значна увага приділяється захисту інформації, у тому числі персональних даних, у мережі Інтернет та інших інформаційних та комп'ютерних системах;

2) наявна розгалужена система законодавства, норми якого містять приписи, що регламентують захист персональних даних працівника, зокрема, визначають правила збору та обробки персональних даних;

3) роботодавець, за згодою потенційного працівника, має право на отримання інфор-

мації з різних інформаційних джерел та уповноважений здійснювати збір різноманітної інформації про працівника.

На відміну від США, у країнах Європи право на захист персональних даних як фундаментальне право та окремий правовий інститут сформувалось набагато пізніше.

Зокрема, зарахування права на захист персональних даних до європейського «каталогу фундаментальних прав» було здійснено на засіданні Рада ЄС у Кельні (Німеччина) 4 липня 1999 р., коли було ухвалено рішення про підготовку проекту Хартії основних прав Європейського Союзу. У зв'язку з цим Робоча група, підтримуючи рішення Ради ЄС, ухвалила 7 вересня 1999 р. рекомендацію, якою запропонувала включити право на захист персональних даних до європейського «каталогу фундаментальних прав» [5, с. 278].

Відтоді на європейському просторі активно приймають спеціальні закони щодо захисту персональних даних особи або вносять зміни до раніше прийнятих законів із метою узгодження їх із новою концепцією ЄС.

Так, наприклад, у Німеччині на базі Закону Землі Гессен 1970 р. був розроблений і прийнятий базовий нормативний акт ФРН «Про подальший розвиток оброблення даних і захисту даних» від 2012 р., який регулює суспільні відносини, що виникають у процесі накопичення, перероблення і використання персоніфікованої інформації (персональних даних) [6, с. 96].

Багато уваги приділено в Німеччині й технічному захисту інформації, на що звертають увагу деякі науковці. Зокрема, як зазначає В. Сідак, в інтересах інформаційної безпеки урядом Німеччини в 1993 р. створено федеральне відомство із забезпечення безпеки у сфері інформаційної техніки. До компетенції цього відомства належать, крім технічного захисту інформації, ще й консультації громадян із питань технічного захисту інформації, а також сертифікація та стандартизація засобів безпеки. Крім того, це відомство займається пропагандою необхідності здійснювати захист інформації на підприємствах [7, с. 8].

Варто також зауважити, що у трудовому законодавстві Франції та Італії поняття персональних даних працівника визначається як інформація, необхідна роботодавцю у зв'язку з трудовими відносинами, що стосується конкретного працівника і пов'язана з його професійною кваліфікацією, діловими, професійними якостями. Ця інформація стосується також вимог, що можуть бути висунуті до працівника у зв'язку з характером роботи. Наведене визначення Р. І. Чанишев пропонує включити до положень КЗпП України. При цьому, як зазначає вчений, закон Франції від 31 грудня 1992 р. про охорону особистої гідності працівника під час наймання на роботу і в період дії трудового договору дає право роботодавцю вимагати при наймі інформацію виключно з метою визначення професійної кваліфікації особи, яка наймається. Вона не має стосуватися його морального обліку, характеру та особливостей особистого і сімейного життя [8, с. 97].

Деякі країни, хоча і не забороняють або не перешкоджають збору даних працівників із джерел третіх сторін, обмежують цю обробку даних роботодавцем.

Наприклад, в Австрії існує гарантоване право отримувати інформацію про працівника від колишнього роботодавця працівника. Це передбачено тим, що так звана довідка (довідка про зайнятість) має стосуватися тривалості трудових відносин та виду послуг. Також будь-яке твердження чи використання фраз, що перешкоджають майбутній кар'єрі працівника, заборонено. Зокрема, інформація не може надаватися наступному роботодавцеві, якщо це стосується зауважень щодо причини звільнення працівника або негативної оцінки його роботи або зайняття діяльністю, наданої членом робочої ради чи членом профспілки. Те саме стосується усних комунікацій (колишніх) роботодавців. Аналогічне правове положення є в Бельгії [9].

Тож, як вбачається з аналізу законодавства деяких європейських держав у сфері захисту персональних даних працівника, у ньому значно обмежені види інформації, які дозволяється вимагати роботодавцю у зв'язку з працевлаштуванням працівника.

В окремих європейських країнах прийнято спеціальні нормативні акти у сфері захисту персональних даних працівника. Наприклад, у Польщі діє Положення про загальний захист даних, який набрав чинності 25 травня 2018 р., що регулює, у тому числі, збирання й обробку персональних даних працівника, включаючи біометричні дані. Відповідно до цього Положення роботодавець має право вимагати певний перелік персональних даних від кандидатів/працівників. Важливо, що роботодавець також має право збирати інші дані, пов'язані з роботою, якщо працівник надає свою згоду та обробку таких даних буде здійснено також і в інтересах самого працівника. Разом із тим Положення також встановлює обмеження на здійснення відеоспостереження за працівниками на підприємстві, а також спеціальні вимоги до зберігання особистих даних. Так, відеоспостереження буде можливим, якщо це необхідно для забезпечення безпеки працівників, захисту майна, контролю виробництва або зберігання таємниці конфіденційної інформації. Кожен роботодавець зобов'язаний вказувати цілі, обсяг та спосіб моніторингу персональних даних працівника у колективному чи трудовому договорі або робочій інструкції [10].

У деяких країнах, зокрема, таких як Хорватія та Чеська Республіка, роботодавці мають повідомити своїх працівників про спостереження та моніторинг роботи електронної пошти. В інших країнах, таких як Болгарія та Польща, це не передбачено за законом, але на практиці роботодавці з метою впровадження політики прозорості щодо їх співробітників включають відповідні умови та правила до правил внутрішнього розпорядку або колективного договору, відповідно, працівники отримують інформацію про можливий моніторинг робочих повідомлень електронної пошти та доступу до інтернету. Зокрема, роботодавцем визначаються такі питання: чи можна використовувати приватні електронні листи під час робочого часу; умови та робота електронної пошти для приватних цілей; яка процедура відкриття електронної пошти працівника у разі тривалої відсутності; чи може працівник отримати доступ до інтернету в робочий час, технічні та організаційні заходи щодо захисту персональних даних, що здійснюються роботодавцем [11, с. 11].

Отже, характерною для багатьох країн Європи є практика, коли роботодавець як власник комп'ютерної системи отримує право здійснювати спостереження за електронними повідомленнями працівника, його електронною поштою, однак таке спостереження може здійснюватися виключно з відома працівника.

При цьому майже в усіх європейських державах діє спеціально утворений орган, до повноважень якого входить здійснення контролю за дотриманням процедур та режимів захисту персональних даних, у тому числі працівників. У Чехії, приміром, це Управління з захисту персональних даних, у Хорватії – Агентство із захисту персональних даних, у Болгарії – Комісія із захисту персональних даних тощо. Найбільш характерними повноваженнями цих інституцій є здійснення нагляду за здійсненням захисту персональних даних, виявлення порушень під час збору персональних даних та застосування санкцій, здійснення моніторингу законодавства про захист персональних даних, розгляд та вирішення скарг тощо.

Висновки. Таким чином, можна зазначити такі особливості правового регулювання захисту персональних даних працівника в державах Європи:

1) як правило, захист персональних даних працівника не виокремлюється в самостійний інститут, а є невід'ємною частиною загального інституту захисту персональних даних;

2) спеціальні норми та положення щодо захисту персональних даних працівника

розробляються роботодавцями у локальних актах – правилах внутрішнього трудового розпорядку, колективних договорах;

3) на законодавчому рівні встановлюються конкретні обмеження щодо видів інформації, яку дозволено роботодавцю вимагати від працівника/кандидата під час прийому на роботу, джерела інформації, які можуть при цьому використовуватися, а також забороняється обробка персональних даних працівника без його прямої згоди;

4) встановлення права роботодавця здійснювати моніторинг та спостереження за електронною поштою, електронними повідомленнями працівника, які розміщені (зберігаються) в інформаційних системах роботодавця.

Анотація

Статтю присвячено дослідженню передового міжнародного досвіду захисту персональних даних працівника. Розглянуті напрацювання у цій сфері деяких країн Європи та США, виявлено особливості інституту захисту персональних даних працівника в США. На підставі проведеного аналізу визначено особливості правового регулювання захисту персональних даних працівника в деяких країнах Європи.

Ключові слова: персональні дані, працівник, захист інформації, трудові правовідносини, міжнародний досвід.

Аннотация

Статья посвящена исследованию передового международного опыта защиты персональных данных работника. Рассмотрены наработки в этой сфере ряда стран Европы и США, выявлены особенности института защиты персональных данных работника в США. На основании проведенного анализа определены особенности правового регулирования защиты персональных данных работника в некоторых странах Европы.

Ключевые слова: персональные данные, работник, защита информации, трудовые правоотношения, международный опыт.

Avramenko A.V. Future international experience protection of personal data of employees

Summary

The article is devoted to the study of advanced international experience in protecting personal data of an employee. The developments in this area of some European countries and the USA are considered, the features of the Institute for the protection of personal data of an employee in the United States have been identified. On the basis of the analysis, the peculiarities of the legal regulation of the protection of personal data of an employee in certain countries of Europe have been identified.

Key words: personal data, employee, information protection, labor relations, international experience.

Список використаних джерел:

1. Крилова Ю. І. Захист персональних даних: вітчизняний та зарубіжний досвід. *Інформація і право.* 2017. № 3 (22). С. 57−63.
2. Теремецький В. І., Цвірюк Д. М. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. *Часопис Академії адвокатури України.* 2014. № 2 (23). Т. 7. С. 73−82.
3. Кравчук М. М. Міжнародний досвід правового регулювання захисту персональних даних у мережі Інтернет. *Наукові записки Інституту законодавства Верховної Ради України.* 2013. № 3. С. 123−126.

4. Венедіктов С. В. Трудовий договір у Сполучених Штатах Америки. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2017. № 45. Т. 1. С. 131−135.
5. Мельник К. Інституційно-правовий захист персональних даних в Європейському Союзі. *Національний юридичний журнал: теорія і практика.* 2014. Вип. 124. Ч. 2. С. 275−280.
6. Борисова Л. В., Тулупов В. В. Захист прав суб'єктів персональних даних. *Форум права*. 2013. № 1. С. 96–100.
7. Сідак В. Організація системи захисту інформації в Німеччині. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2006. Вип. 2 (13). С. 7−10.
8. Чанишев Р. І. Інформація про персональні дані працівника та її захист. *Актуальні проблеми держави і права*. 2010. Вип. 52. С. 94−99.
9. Hendrickx F. Protection of workers' personal data in the European Union. URL: http://ec.europa.eu/social/BlobServlet?docId=2507&langId=en.
10. Synowiec M. Poland: GDPR Implementation. *DLA Piper.* 2018. URL: https://knowledge.dlapiper.com/dlapiperknowledge/globalemploymentlatestdevelopments/poland-gdpr-implementation.
11. Privacy protection in the workplace: Vinci Partnership Project "Raising awareness of the data protection issues among the employees working in the EU". 2012. URL: https://www.uoou.cz/assets/File.ashx?id_org=200156&id_dokumenty=1168.