

УДК 349.2

А. В. Авраменко

ПРИНЦИПИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ

Постановка проблеми. Виходячи з положень статей 3 та 21 Конституції України, які визначають природне право початком та основою української правової системи, державне управління передбачає наявність двох головних аспектів: правоохоронного, який полягає у можливості реалізації прав та свобод людини, та правозахисного щодо захисту порушених суб'єктивних прав. Мета захисту – припинення правопорушення та відновлення бажаних для людини, суспільства або держави прав та свобод, встановлених нормативно-правовим актом чи договором. Ці та інші дії спираються на комплекс основоположних ідей та засад, які в правовій науці називаються принципами.

Актуальність теми дослідження підтверджується недостатністю кількості наукових робіт, які засновані на оновленому законодавстві та новітніх концепціях, які присвячені захисту персональних даних працівників та удосконаленню принципів у цій сфері.

Стан дослідження. У вітчизняній науці трудового права проблемам принципів захисту персональних даних працівника присвячено недостатньо наукових робіт. Деякі аспекти означеної проблематики зачіпали у своїх працях такі науковці, як В.С. Венедіктов, В.М. Колодій, М.В. Різак, В.С. Політанський, І.М. Сопілко, О.В. Старчук та інші. Водночас, у наявних наукових працях принципи захисту персональних даних працівника розглядаються фрагментарно, а комплексні дослідження у даній сфері майже відсутні.

Саме тому, **метою статті** є характеристика принципів захисту персональних даних працівників.

Виклад основного матеріалу. Механізм захисту персональних даних працівника ґрунтується на певній системі принципів, завдяки яким такий механізм набуває демократичного характеру та стає соціально орієнтованим. Іншими словами, принципи захисту персональних даних відбивають засадничі соціально-демократичні ідеї, що лежать в основі відповідного механізму; навіть більше, принципи є одним з його елементів. Відтак, дослідження питання щодо принципів захисту персональних даних надасть змогу визначити ідейно-правову сутність механізму захисту персональних даних працівника.

З цього приводу варто погодитись з думкою В.М. Колодія, який зазначає, що принципи права – це ідеологічна категорія, а це означає, що вони, як і право загалом, є формою суспільної свідомості, яка здійснює ідейний, інформаційно-виховний вплив загального характеру, тобто виконує функцію загального закріплення суспільних відносин, що та дає можливість розглядати їх з позиції певних ідей, керівних засад [1, с. 41].

Поняття «принципи» вживається головним чином у значенні ідей, ціннісних орієнтирів, керівних засад, які визначають сутність та відбивають специфіку тієї чи іншої сфери соціальних відносин. За допомогою принципів певні явища,

правовідносини, суспільна діяльність набувають сутнісних особливостей відповідної історичної епохи та соціально-правової системи, що прийнята у державі.

Різноманітність правових принципів потребує їх певної систематизації та класифікації за визначеними критеріями. З цього приводу у науковій літературі висувається ряд пропозицій, однак, однією з найбільш розповсюджених наукових концепцій є класифікація принципів права за галузевим критерієм. За даним критерієм принципи права поділяються на загальногалузеві, міжгалузеві та спеціально галузеві.

Зважаючи на комплексний характер правовідносин, що виникають у сфері захисту персональних даних, принципи, на яких ґрунтується такі правовідносини також мають міжгалузевий комплексний характер. Зокрема, комплексність досліджуваного виду правовідносин виражається у тому, що вони регламентуються законодавством, що належить до декількох галузей права, основними з яких є інформаційне та трудове право. Відтак, принципи захисту персональних даних працівника містять засадничі основи обох галузей права. При цьому, слід також вказати на існування загальних принципів, притаманних праву.

Традиційно до системи загальних принципів відносяться: верховенство права, законності, пріоритетності життя, здоров'я, особистої безпеки людини та громадянина, особистої недоторканності особи, демократизму, народовладдя тощо.

Що стосується галузевих принципів, то вони різняться залежно від галузі права. Так, І.І. Швидкій до основних принципів правового регулювання трудових відносин працівників відносить: 1) професіоналізм при здійсненні своїх трудових зобов'язань; 2) компетентність; 3) дисципліна й законність; 4) персональна відповідальність за невиконання або неналежне виконання трудових зобов'язань; 5) розмежування компетенції між працівниками різної кваліфікації; 6) оплата праці за трудову діяльність на рівні не нижчому за встановлений рівень мінімальної заробітної плати; 7) свобода й добровільність праці; 8) договірний характер найманої праці; 9) визначеність трудової функції [2, с. 14–15].

Зі свого боку до принципів інформаційного права науковці відносять: 1) свободу одержання та поширення інформації; 2) об'єктивність, вірогідність, повноту та точність інформації; 3) гармонізацію інтересів особи, суспільства та держави в інформаційній діяльності; 4) мінімізацію негативного інформаційного впливу; 5) мінімізацію негативних наслідків функціонування інформаційних технологій; 6) недопущення несанкціонованого поширення, використання та знищення інформації; 7) приналежність інформації до об'єктів цивільних правовідносин, її вільний обіг у визначених законом випадках; 8) єдність та різниця інформації та носія інформації; 9) об'єктивність надання інформації; 10) первинність створення інформації; 11) обмеження доступу до інформації у визначених випадках; 12) взаємну гармонізацію інформаційного права та всієї системи вітчизняного законодавства [3, с. 9–14].

Таким чином, система принципів трудового та інформаційного права включає загальні принципи, на яких ґрунтується уся галузь права, та спеціальні, на яких засновані окремі інститути та правовідносини, що виникають у межах відповідної галузі.

Деякі з визначених науковцями принципів знайшли своє безпосереднє закріплення в нормативно-правових актах, інші ж слідують зі змісту правових норм. Так, відповідно до Закону України «Про інформацію» основними принципами інформаційних відносин є: гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; вірогідність та повнота інформації; свобода вираження поглядів та переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя [4].

Закон України «Про захист персональних даних» [5] не містить окремої статті, яка присвячена принципам правовідносин із захисту персональних даних. Однак, виходячи зі змісту положень норм даного Закону, можна зазначити, що такими принципами є: конфіденційність інформації, що становить персональні дані особи; недопущення збирання, накопичення та використання інформації про особу без її згоди тощо. Чинний Кодекс законів про працю (далі – КЗпП) України також не визначає принципи трудових правовідносин.

На підставі проведеного вище аналізу, можемо виокремити такі принципи захисту персональних даних працівника:

1. Принцип добровільності надання персональних даних особою під час влаштування на роботу.

Зміст даного принципу полягає у тому, що збір інформації про працівника (потенційного працівника) здійснюється роботодавцем або третіми особами виключно на підставі прямої та однозначної згоди особи щодо такого збору. При цьому, згода працівника (потенційного працівника) на збір інформації про нього у разі, якщо він самостійно подає документи, які відповідно до частини 4 статті 6 Закону України «Про захист персональних даних» є первинними джерелами відомостей про фізичну особу (видані на її ім'я документи, підписані нею документи, відомості, які особа надає про себе), згода такого працівника презюмується лише у відношенні конкретно обраного роботодавця (до якого подаються документи з метою працевлаштування) або для конкретної мети (працевлаштування). У інших випадках обов'язковою є письмова згода суб'єкта персональних даних;

2. Принцип вірогідності та повноти інформації, що складає персональні дані працівника.

Даний принцип у науковій літературі визначається не лише, як спеціальний принцип інформаційних правовідносин, а й однією з ключових вимог щодо інформації та захисту інформації взагалі. При цьому вірогідність інформації є досить істотним принципом інформаційних відносин та основоположною вимогою щодо інформації, у зв'язку з чим потребує свого законодавчого визначення у Законі України «Про інформацію», зокрема, у такому формулюванні як відповідність, адекватність та ідентичність отриманих даних фактичним умовам або є властивістю інформації, яка визначає ступінь об'єктивного, точного зображення подій, фактів, що мали місце [6, с. 57].

У контексті обробки персональних даних про працівника дотримання даного принципу обумовлено особливою важливістю мети, з якою здійснюється збір та обробка персональних даних. За загальним правилом відповідальність за вірогідність

персональних даних несе особа, яка подає такі дані. Разом з тим, обов'язком роботодавця є перевірка вірогідності та повноти поданої інформації, яка складає персональні дані працівника. Крім того, важливо згадати про те, що за вірогідність та повноту тих даних, які формуються роботодавцем у ході виконання працівником трудової функції (відомості про заробітну плату, здійсненні відрахування до фонду загальнообов'язкового державного соціального страхування тощо) відповідальність перед третіми особами (органами державної фіскальної служби, органами Пенсійного фонду тощо) та працівником несе відповідальність роботодавець;

3. Принцип адекватності, достатності та ненадмірності збору та обробки персональних даних працівника.

Даний принцип відповідає принципу Європейського союзу (далі – ЄС) щодо пропорційності захисту публічного та особистого інтересу особи та означає, що будь-які вимоги роботодавця щодо необхідності представлення працівником (потенційним працівником) інформації про себе мають бути обґрунтованими конкретною необхідністю, яка відповідає меті збору та обробки персональних даних.

У якості порушення даного принципу деякі науковці наводять практичну ситуацію – запровадження роботодавцями процедури ідентифікації персоналу з використанням відбитків пальців. Відцифровані відбитки пальців повинні у такому випадку зберігатися в окремому реєстрі володільця. Метою обробки було забезпечення реалізації обов'язків роботодавця, а саме підтримання трудової дисципліни та створення належних умов праці, забезпечення пропускового режиму на підприємстві. При цьому, як зазначають науковці, на практиці з цього приводу надходить чимала кількість скарг. Зокрема, заявники скаржаться на примусовий характер впровадження таких систем, які супроводжуються погрозами з боку роботодавців звільнити тих працівників, хто не погоджується надати відбитки пальців [7, с. 46]. У цьому зв'язку слід зазначити, що згідно із визначенням терміну «біометричні дані», що міститься в Законі України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» [8] відцифровані відбитки пальців рук є біометричними даними.

Відтак, достатність та ненадмірність таких заходів значною мірою обумовлена видом діяльності підприємства, установи або організації та визначається з урахуванням співвідношення можливих негативних наслідків для роботодавця, якщо працівник відмовиться від надання таких даних про себе, та для працівника, якщо роботодавець не забезпечить їх належне зберігання та схоронність;

4. Принцип відповідальності роботодавця за стан збереження та забезпечення захисту персональних даних працівника.

Даний принцип означає, що за стан збереженості персональних даних працівника, які зібрані та зберігаються у роботодавця або за його замовленням третіми особами, несе відповідальність роботодавець. Так само, останній несе відповідальність за несанкціоноване використання даних працівника, рівень безпеки зберігання даних в інформаційних системах тощо.

О.В. Олійник вказує також на принцип комплексного підходу до організації забезпечення інформаційної безпеки, який передбачає створення органічно

взаємозв'язаної сукупності сил, засобів та спеціальних методів, спрямованих на забезпечення безпеки інформації, що підлягає захисту та сфери її обігу [9, с. 172]. Даний принцип, на нашу думку, є невіддільним елементом принципу відповідальності роботодавця за стан збереження та забезпечення захисту персональних даних працівника.

Для забезпечення схоронності та недопущення несанкціонованого використання персональних даних працівника роботодавець має забезпечити надійність інформаційно-телекомунікаційних систем, у яких зберігаються такі данні, а також недоступність інформації для сторонніх осіб, яка зберігається на паперових носіях чи інших джерелах інформації;

5. Принцип безперервності забезпечення захисту персональних даних працівника.

Принцип безперервності забезпечення інформаційної безпеки, на думку М.В. Бем, І.М. Городиського та інших, полягає у повсякденному (безперервному) застосуванні як загальних, так та спеціальних засобів та методів забезпечення інформаційної безпеки на всіх її етапах життєвого циклу [7, с. 173].

У відношенні до захисту персональних даних працівника цей принцип також означає, що роботодавець має визначити відповідальну особу за зберігання персональних даних працівників, встановлення належної системи безпеки тощо;

6. Принцип використання персональних даних працівника роботодавцем виключно з метою забезпечення виконання працівником трудової функції та виконання роботодавцем своїх повноважень.

Як вже згадувалось раніше, добровільність збирання та обробки персональних даних працівника, які подані особою самостійно у процесі працевлаштування та сформовані роботодавцем у ході виконання працівником трудової функції, презюмується лише у випадку, якщо відповідне збирання та обробка здійснюються із заздалегідь визначеною метою – забезпечення трудової дисципліни, належного виконання працівником трудової функції та реалізації роботодавцем своїх повноважень у відносинах з державною фіскальною службою, іншими органами.

У зв'язку з цим у науковій літературі наголошується, що якщо особа надала згоду на обробку персональних даних, які по своїй суті непотрібні для досягнення поставленої мети обробки, така обробка розглядатиметься як непропорційна та становитиме порушення законодавства про захист персональних даних [7, с. 46–47];

7. Принцип відкритості та прозорості використання роботодавцем персональних даних працівника.

Даний принцип означає, що обробка персональних даних працівника здійснюється відкрито для самого працівника, тобто, працівник має право у будь-який час звернутися до роботодавця для отримання актуальної інформації про себе, яка зберігається у роботодавця. Крім того, працівник має право знати для якої мети обробляються його персональні дані, які треті особи мають до них доступ тощо, для чого роботодавець має повідомляти по це працівника. Суб'єкт даних повинен мати право доступу до персональних даних, які збирають щодо нього, та реалізовувати таке право вільно та через розумні проміжки часу для того, щоб бути обізнаним про законність опрацювання та перевірити її.

Принцип прозорості вимагає, щоб будь-яка інформація, призначена для громадськості або суб'єкта даних, була стислою та зрозумілою, з використанням чітких та простих формулювань, а також, за необхідності, із застосуванням засобів візуалізації. Таку інформацію можна надавати в електронному форматі, наприклад, через веб-сайт, коли її адресовано громадськості. Це, зокрема, є доцільним у ситуаціях, коли збільшення кількості агентів та технологічна складність практичної діяльності перешкоджають обізнаності та розумінню суб'єкта даних того, чи збирають її або його персональні дані, хто їх збирає та для якої цілі, як, наприклад, у випадку онлайн-реклами [10];

8. Принцип чіткості визначення мети збору та використання персональних даних працівника.

За загальним правилом збір та обробка персональних даних працівника здійснюється з метою забезпечення виконання працівником його трудової функції належним чином, а також реалізації роботодавцем своїх повноважень. Разом з тим, у випадку, якщо обробка персональних даних здійснюється також із іншою метою, остання має бути чітко сформульована для того, щоб згода на таку обробку була надана працівником в однозначній формі;

9. Принцип виключності випадків обмеження прав працівника при обробці його персональних даних.

Випадки обмеження прав суб'єкта персональних даних, зокрема, надання персональних даних працівника на запит третіх осіб, обробка персональних даних для інших цілей без згоди працівника, визначені у статті 25 Закону України «Про захист персональних даних».

У цій статті зазначається, що обмеження дії статей 6, 7 та 8 цього Закону може здійснюватися у випадках, які передбачені законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав та свобод суб'єктів персональних даних чи інших осіб [5].

Узагальнюючи випадки обмеження прав суб'єкта персональних даних, М.В. Бем, І.М. Городиський та інші виокремлюють такі умови відповідних обмежень: 1) передбачене законом; 2) необхідне/пропорційне; 3) переслідує одну з легітимних цілей – національної безпеки, економічного добробуту або захисту прав та свобод суб'єктів персональних даних чи інших осіб [7, с. 99].

Крім того, дозволяється обробка персональних даних без застосування положень цього Закону, якщо така обробка здійснюється: 1) фізичною особою виключно для особистих чи побутових потреб; 2) виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів [5]. Така обробка може здійснюватися виключно за умови знеособлення персональних даних.

Використання персональних даних працівниками суб'єктів відносин, пов'язаних із персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків, що виключає розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків [11, с. 100].

Висновки. Таким чином, розглянуті вище принципи захисту персональних даних працівника складають фундаментальні засади, на яких функціонує механізм захисту персональних даних.

Література:

1. Колодій В.М. Принципи права : генеза, поняття, класифікація та реалізація. *Альманах права*. 2012. Вип. 3. С. 42–46.
2. Швидкій І.І. Особливості правового регулювання праці працівників ДАІ як суб'єктів трудових правовідносин : автореф. дис. канд. юр. наук : спец. 12.00.05 «Трудове право; право соціального забезпечення». Луганськ, 2009. 21 с.
3. Баранов О. Система принципів інформаційного права. *Правова інформатика*. 2006. № 2 (10). С. 5–15.
4. Про інформацію : Закон України від 02 жовтня 1992 р. № 2657-ХІІ. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.
5. Про захист персональних даних : Закон України від 01 червня 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.
6. Політанський В.С. Принципи інформаційно-правових відносин. *Часопис Київського університету права*. 2013. № 1. С. 55–60.
7. Вем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних : Правове регулювання та практичні аспекти: науково-практичний посібник. Київ : К.І.С., 2015. 220 с.
8. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20 листопада 2012 р. № 5492-VI. URL: <http://zakon.rada.gov.ua/laws/show/5492-17>.
9. Олійник О.В. Принципи забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського університету. Серія «Право»*. 2012. Вип. 18. С. 170–173.
10. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних та про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) : Регламент Європейського парламенту та Ради від 27 квітня 2016 р. № 2016/679. URL: <https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf>.
11. Борисова Л.В., Тулупов В.В. Захист прав суб'єктів персональних даних. *Форум права*. 2013. № 1. С. 96–100.

Анотація

Авраменко А. В. До питання щодо особливостей державної служби в Україні. – Стаття.

Статтю присвячено дослідженню принципів захисту персональних даних працівника. У статті розглянуто поняття принципів та здійснено їх класифікацію на загальногалузеві, міжгалузеві та спеціально галузеві. На підставі проведеного аналізу виокремлено принципи захисту персональних даних працівників.

Ключові слова: інформація, принципи права, персональні дані, працівник, захист, трудові правовідносини.

Аннотация

Авраменко А. В. К вопросу об особенностях государственной службы в Украине. – Статья.

Статья посвящена исследованию принципов защиты персональных данных работника. В статье рассмотрены понятия принципов и осуществлена их классификация на общеотраслевые, межотраслевые и специально отраслевые. На основании проведенного анализа выделены принципы защиты персональных данных работников.

Ключевые слова: информация, принципы права, персональные данные, работник, защита, трудовые правоотношения.

Summary

Abramenko A. V. On the issue of the peculiarities of civil service in Ukraine. – Article.

The article is devoted to research of principles of protection of the personal data of the employee. The concept of principles is considered and their classification is made on the general-branch, inter-branch and special-purpose branches. On the basis of the analysis, the principles of protection of personal data of employees are singled out.

Key words: information, principles of law, personal data, employee, protection, labor relations.