by the relevant law. It has been proven that according to the Law of Ukraine «On Prevention of Corruption», notaries are classified as persons who provide public services and are subject to requirements for the prevention and settlement of conflicts of interest. At the same time, the limits of private interest that a notary must take into account when performing notarial actions are much wider than those established in a special law. It is noted that the Law «On Notaries» is not the only normative legal act that defines its own rules regarding the sphere of private interest during the performance of professional duties related to the provision of public services, similar narrowed legal regulation of this restriction is also contained in the laws , which regulate the activities of public and private contractors, appraisers, auditors and other persons who provide public services.

Based on the analysis of the norms of the Law of Ukraine «On Notaries» it is proved that the restriction on the right to perform notarial acts concerns only the personal and, in part, family relations of the notary, which are associated with a conflict of interests at the level of departmental legal regulation in terms of violation of the rules of professional ethics, in while the provisions of the Law of Ukraine «On Prevention of Corruption» apply to the notary public, whose private interest is much broader than that declared in the relevant law, which does not contribute to a clear understanding of situations when a notary public has refrain from performing notarial acts. Taking into account the above, specific changes are proposed to the Law of Ukraine «On Notaries» in order to bring it into line with the provisions of the anti-corruption legislation.

***Keywords*:** *restrictions on the right to perform notarial acts, notarial acts, notarial activity, personal interest, private interest.*

УДК 349.2
DOI: 10.31733/2078-3566-2023-2-171-178

Ганна СПІЦИНА©
доктор
юридичних наук,
професор

Світлана ГУЦУ©
кандидат
юридичних наук,
доцент

*(Національний аерокосмічний університет
ім. М. Є. Жуковського "ХАІ", м. Харків, Україна)*

ЗАХИСТ ОСОБИСТОЇ ІНФОРМАЦІЇ ПРАЦІВНИКІВ, ОТРИМАНОЇ У ПРОЦЕСІ ВІДЕОСПОСТЕРЕЖЕННЯ НА РОБОЧОМУ МІСЦІ

Досліджено стан правового регулювання захисту персональних даних працівників, зібраних у процесі моніторингу і відеоспостереження на робочому місці. Встановлено, що національне трудове законодавство не має спеціальних норм щодо особливостей регулювання цього питання. Натомість у європейських країнах є доволі суттєві напрацювання і нормативна база у сфері використання таких методів роботи з персональною інформацією. Автори пропонують доповнити національне законодавство визначенням правил, підстав і строків здійснення роботодавцем моніторингу і відеоспостереження на робочому місці. Це дозволить захистити інтереси сторін трудових правовідносин і сприятиме виконанню законодавства у сфері захисту персональних даних.

Ключові слова: *особиста інформація, спостереження на робочому місці, обробка персональних даних працівника, персональні дані працівників, інформація, захист інформації, трудові правовідносин, працівник, роботодавець, трудовий договір.*

© Г. Спіцина, 2023
ORCID iD: https://orcid.org/0000-0001-9131-0642
spitsyna_hanna@ukr.net

© С. Гуцу, 2023
ORCID iD: https://orcid.org/0000-0003-1373-6079
s.gutsu@khai.edu

Постановка проблеми. З розвитком штучного інтелекту, баз даних, Інтернету такі технології, як відеоспостереження, зберігання та обробка персональної інформації постійно розширяються і вдосконалюються. Відеоспостереження на робочому місці – це діяльність роботодавців, спрямована на збирання інформації щодо поведінки працівників за допомогою камер, комп'ютерів, приладів стеження та інших засобів у робочий час і на робочому місці. Загалом спостереження на робочому місці розглядається як форма реалізації права роботодавця на управління та контроль, котрий може допомогти підвищити ефективність роботи, оптимізувати робочі процеси та зменшити ризики на робочому місці. Однак на практиці роботодавці часто зловживають відеоспостереженням на робочому місці, наприклад, для проведення службових та внутрішніх розслідувань. Це може спричинити обмеження законних прав та інтересів працівників і загрожувати безпеці їхньої особистої інформації. Зі зростанням культури дистанційної та гібридної роботи ця проблема набуває ще більшої актуальності бо роботодавці все частіше звертаються до різних методів моніторингу співробітників.

Метою дослідження є аналіз вітчизняного і європейського законодавства у сфері захисту персональних даних працівника, зібраних у процесі моніторингу і відеоспостереження.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. На жаль, на сьогодні комплексні дослідження, присвячені питанню правового регулювання захисту персональних даних працівника, отриманих під час моніторингу з боку роботодавця, відсутні. У сучасній науці трудового права окремі питання захисту персональних даних працівника знайшли відображення у працях таких вчених: М. Грекової, В. Жернакова, Є. Краснова, К. Мельника, С. Прилипка, О. Ярошенка, А. Чернобай. Однак наразі вказана тема залишається актуальною та не до кінця дослідженою.

Виклад основного матеріалу. Питання захисту персональних даних виникають у повсякденному житті кожної людини – під час взаємодії з державними органами влади, органами місцевого самоврядування, судовими, правоохоронними органами, у закладах охорони здоров'я, під час купівлі товарів, отримання послуг, подорожування та навіть користування мережею Інтернет. Звичайно, у процесі трудових відносин також неможливо уникнути збору, використання, обробки і зберігання інформації, що містить персональні дані працівників. Але в окремих випадках роботодавці цілеспрямовано впроваджують додаткові заходи щодо отримання таких даних.

Згідно з опитуванням ExpressVPN, 78% роботодавців погодилися використовувати інструменти моніторингу своїх співробітників [1]. В іноземній літературі під моніторингом працівників розуміють використання роботодавцем різних методів спостереження та збору даних, як-от: програмне забезпечення для моніторингу працівників, ключ-карти, біометричні дані та інші методи електронного моніторингу. Сьогодні роботодавцями широко використовуються такі методи електронного моніторингу:

1. Використання програмного забезпечення, котре дозволяє працівникам вмикати або вимикати його під час початку/закінчення офісної або віддаленої роботи;
2. Використання камер відеоспостереження, розміщених на помітних місцях у спільних приміщеннях;
3. Моніторинг робочих станцій компанії із попереднім інформуванням працівників;
4. Запис телефонних розмов за згодою учасників.

Щодо правового регулювання цієї сфери, то міжнародним співтовариством вже накопичено доволі суттєвий досвід і законодавчу базу. Так, у США ще у 1906 р. було прийнято перший закон «Про захист інформації», проте інтенсивний розвиток відповідного законодавства розпочався тільки після появи комп'ютерної техніки. В Європі персональні дані захищають приблизно півсторіччя. В Україні – з 1 січня 2011 р., коли набув чинності Закон України «Про захист персональних даних» від 01.06.2010. Він регулює всі правові відносини, пов'язані із захистом та обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя у зв'язку з обробкою персональних даних.

Відповідно до українського законодавства персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Термін «персональні дані» стосується лише фізичних осіб [2]. У

роз'ясненні Мінюсту «Деякі питання практичного застосування Закону України «Про захист персональних даних»« від 21.12.2011 [3] зазначено, що законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, що є персональними даними, задля можливості застосування положень Закону до різноманітних ситуацій, в тому числі при обробці персональних даних в інформаційних (автоматизованих) базах та картотеках персональних даних, що можуть виникнути у майбутньому, у зв'язку зі зміною в технологічній, соціальній, економічній та інших сферах суспільного життя. Отже, Мінюст визнав наявність проблеми, але не дав відповіді на запитання, які саме відомості дозволяють ідентифікувати фізичну особу. За вказаних обставин законодавець не визначає вичерпного переліку відомостей, що належать до персональних даних. Але орієнтовний перелік персональних даних визначив Конституційний Суд України у своєму рішенні № 2-рп/2012 від 20.01.2012, відповідно до якого інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовій, інтимній, товариській, професійній, діловій та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їхньою згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Перелік даних про особу, що визнаються як конфіденційна інформація, не є вичерпним [4].

Персональні дані поділяються за критерієм їхньої «чутливості» на: загальну інформацію (наприклад, ПІБ, дата і місце народження, громадянство, місце проживання тощо) та «чутливі» дані (стан здоров'я, етнічне походження, віросповідання, ідентифікаційні номери, відбитки пальців, аудіо-, відео-, фотофіксація, судимість та ін.). Для «чутливих» персональних даних передбачається більш високий ступінь захисту. Забороняється збирання, зберігання, використання та передавання без згоди суб'єкта, як правило, саме чутливих персональних даних [5].

Відповідно до Основного закону ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [6].

На жаль, у трудовому законодавстві України взагалі відсутнє правове регулювання захисту персональних даних працівників, хоча актуальність цього питання зумовлюється тим, що при прийомі на будь-яку роботу та у процесі трудової діяльності працівник повинен надати роботодавцеві власні персональні дані, а саме: відомості про саму особу, її освіту, сімейний стан, стаж роботи, а в деяких випадках – відомості про доходи за минулий рік тощо. Однак проєкт Трудового кодексу України усуває цю прогалину. Зокрема, в ньому містяться норми, що регулюють питання, пов'язані із захистом персональних даних працівників, як-от: встановлена заборона роботодавцю надавати третім особам будь-яку інформацію про причини звільнення та інші відомості про працівника, крім надання їх на прохання працівника та в інших випадках, передбачених законом; відомості про оплату праці працівника віднесено до конфіденційної інформації, що надається будь-яким органам чи особам лише у випадках, передбачених законом, або за згодою чи на вимогу працівника; визначена відповідальність роботодавця за заподіяння моральної шкоди тощо [7].

Вчена А. Чернобай наголошує, що поняття персональних даних працівника є вужчим за поняття персональних даних особи, оскільки йдеться не про всі відомості (факти, події, обставини приватного життя особи тощо), а лише про такі обставини, що характеризують фізичну особу як працівника. Персональні дані працівника слід розглядати як інформацію, отримання якої необхідно роботодавцю щодо кожного працівника у зв'язку з трудовими відносинами [8].

Західні дослідники зазначають, що роботодавці можуть законно контролювати

майже все, що робить працівник на роботі, якщо причина моніторингу є достатньо важливою для бізнесу. Роботодавці можуть встановлювати відеокамери, читати пошту, у тому числі електронну, контролювати використання телефону та комп'ютера, використовувати GPS-відстеження тощо. Так, роботодавці в ЄС мають право контролювати працівників на роботі, якщо є законний діловий інтерес. При цьому вкрай важливо збалансувати право роботодавця на законний контроль та управління робочим процесом і право працівника на приватність. Працівник має право бути повідомленим перед проведенням будь-якого моніторингу. Пряма згода потрібна не завжди, але в деяких випадках вона є обов'язковою. Найголовніше, процес моніторингу має відповідати Загальному регламенту захисту даних ЄС (GDPR) [9]. GDPR стверджує, що згода, прозорість і захист даних є важливими. Ці правила застосовуються до організацій (державних і приватних) в ЄС і тих, що знаходяться за межами ЄС і пропонують послуги ЄС. Суть полягає в тому, що моніторинг має бути розумним, а роботодавці повинні враховувати право працівника на конфіденційність. Відповідно до GDPR співробітники повинні бути повідомлені про те, що за ними стежать, стосовно мети моніторингу, строку зберігання отриманих даних і про те, хто має доступ до даних, що відстежуються. Використання прихованого відеоспостереження вважається порушенням ст. 8 Європейської конвенції з прав людини. Також заборонено моніторинг у «чутливих» зонах, таких як туалети, релігійні приміщення та кімнати відпочинку.

Багато країн ЄС вимагають від роботодавців інформувати своїх працівників і обговорювати будь-які проблеми процесу моніторингу перед його проведенням. Робоча група із захисту даних у ст. 29 (WP249) підкреслює, що прозорість повинна застосовуватися до обробки даних на роботі. Працівники мають знати про моніторинг, мету, з якою збираються персональні дані, та будь-яку іншу інформацію, необхідну для забезпечення доцільності такої обробки. У ЄС сформовано два правові підходи до прав на спільне прийняття рішень. У деяких країнах працівники мають право погоджуватися на моніторинг чи ні. В інших – їх необхідно повідомити про моніторинг, але згода не потрібна. Наприклад, у Данії колективні договори часто вимагають від роботодавців інформувати працівників про будь-які заходи моніторингу не пізніше, ніж за шість тижнів до виконання угоди, за винятком випадків, коли мета заходів моніторингу буде перешкоджати попередньому повідомленню. У Чеській Республіці працівники також повинні бути належним чином проінформовані про обробку персональних даних і спеціальні методи моніторингу, у тому числі відеоспостереження. Проте в окремих випадках роботодавцям дозволяється відслідковувати серйозні правопорушення працівників, щоб захистити бізнес. У Фінляндії Закон про захист приватного життя на роботі встановлює суворі умови для використання камер спостереження на робочому місці. Перед початком відеоспостереження необхідно проконсультуватися з працівниками та повідомити їх про це, а в місцях, де розташовані камери, повинно бути помітне сповіщення. Наводити камери на робочі місця взагалі заборонено, але в окремих випадках це дозволяється, наприклад, якщо це необхідно для запобігання або розслідування майнових злочинів. Проте працівники повинні бути проінформовані про розташування спрямованих камер. В Угорщині законодавство визначає деякі основні аспекти відеоспостереження, але залишає більшість особливостей відкритими для тлумачення. В Латвії вимога щодо інформування працівників про будь-яку обробку даних базується на ст. ст. 13 і 14 GDPR, а також на положеннях закону Латвії про обробку даних. Закон Литви про правовий захист персональних даних передбачає, що працівники повинні бути проінформовані в письмовій формі про відео- та голосовий моніторинг на робочому місці. У Польщі з травня 2019 року діють суворі положення, що визначають, коли саме дозволяється моніторинг працівників і як його мають проводити роботодавці. Приховане відеоспостереження за працівниками може бути важко захистити, оскільки, згідно з відповідними законодавчими положеннями, всі без винятку працівники повинні бути поінформовані, що за ними стежать. Згідно зі Словацьким трудовим кодексом роботодавці можуть контролювати працівників лише за таких обставин:

- є поважна причина з огляду на характер діяльності роботодавця;
- намір роботодавця контролювати працівників заздалегідь обговорено з представниками працівників;
- працівників поінформовано про спосіб та обсяг моніторингу.

У Швеції приватним компаніям або державним органам, що здійснюють

відеоспостереження за межами громадських місць, не потрібно отримувати дозвіл, але при цьому мають застосовуватися вимоги GDPR. Якщо приватна організація або державний орган зв'язані колективним договором, вони повинні домовитися про нагляд з відповідною профспілкою, перш ніж його можна буде здійснювати. Якщо за працівником здійснювався контроль, він все одно зможе вимагати відшкодування збитків на основі статті 82 GDPR, навіть якщо його звільнення було законним [10].

Згідно з Директивою 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», держави-члени передбачають, що персональні дані можуть оброблятися тільки за умови, що (a) суб'єкт даних недвозначно дав свою згоду або обробка необхідна для: (b) виконання контракту, стороною якого є суб'єкт даних, чи для вживання заходів на прохання суб'єкта даних до підписання контракту; (c) дотримання правового зобов'язання, яким зв'язаний контролер; (d) захисту життєво важливих інтересів суб'єкта даних; (e) виконання завдання, що здійснюється в суспільних інтересах, чи при виконанні офіційних повноважень, котрими наділений контролер або третя сторона, якій надаються дані; (f) забезпечення законних інтересів, переслідуваних контролером чи третьою стороною або сторонами, для яких надаються дані, крім випадків, коли над такими інтересами переважають інтереси основних прав і свобод суб'єкта даних, що вимагають захисту згідно з п. 1 ст. 1.

Сучасний європейський підхід до обробки персональних даних може бути викладений у вигляді таких принципів: 1) законність, справедливість та прозорість – персональні дані повинні оброблятися законно, справедливо та прозоро. Будь-яку інформацію про мету, методи та обсяги обробки персональних даних слід викладати максимально доступно та просто; 2) обмеження застосування – персональні дані необхідно збирати та використовувати виключно з метою, що була заявлена підприємством (або онлайн-сервісом); 3) мінімізація даних – забороняється збирати особисті дані в більшому обсязі, ніж той, що потрібен для досягнення мети обробки; 4) точність – особисті дані, що є неточними, повинні бути видалені або виправлені (за вимогою користувача); 5) обмеження зберігання – персональні дані мають зберігатися у формі, що дозволяє ідентифікувати суб'єкти даних на строк не більше, ніж це необхідно для досягнення мети обробки; 6) цілісність та конфіденційність – при обробці даних працівників і клієнтів підприємство зобов'язане забезпечити захист персональних даних від несанкціонованої або незаконної обробки, знищення та пошкодження.

Роботодавці обробляють персональні дані своїх працівників щодня та з різною метою. Дані можуть стосуватися виплат працівникам заробітної плати, відпускних, обліку лікарняних, виплат у зв'язку з вагітністю та пологами, оцінки результатів і якості роботи тощо. Будь-яка обробка персональних даних працівника повинна виконуватися тільки для конкретно встановленої мети. Фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки (якщо інше не визначено законом), вважається володільцем персональних даних відповідно до вимог Закону. Тобто в даному випадку володільцем персональних даних є роботодавець, а сам працівник є суб'єктом персональних даних.

З метою безпосередньої реалізації трудових відносин будь-яке підприємство, установа чи організація збирає, накопичує, зберігає, змінює, знищує відомості про своїх працівників у своїх картотеках, базах даних чи спеціальних інформаційних програмах. Відомості про працівників роботодавцем, як правило, зберігаються в особових справах, розроблених інформаційних кадрових програмах, тобто йде мова про накопичення бази персональних даних та її зберігання. Також законодавець виокремлює розпорядника персональних даних – це фізична чи юридична особа, якій володільцем або законом надано право обробляти ці дані від імені володільця. Розпорядник може обробляти персональні дані лише з метою і в обсязі, визначених у договорі з володільцем. Розпорядники на підприємстві є не завжди. До них належать: консультант по кадрам, відділ кадрів на підприємстві, спеціалісти кадрової служби, консалтингова фірма тощо.

При роботі з наведеною інформацією важливо дотримуватися головних принципів захисту персональних даних: роботодавець і спеціалісти кадрової служби несуть відповідальність за збереження персональних відомостей та носіїв, на яких вони зберігаються; має бути організована чітка дозвільно-розмежувальна система доступу до персональних даних для керівників (усіх рівнів) та інших працівників; має здійснюватися регулярний контроль електронних та паперових документів, баз та справ

у кадровій службі та у відповідних структурних підрозділах підприємства.

Однак моніторинг процесу праці, внаслідок якого роботодавець отримує інформацію про працівника, потребує правового вирішення низки питань. Насамперед, тут варто відзначити відсутність чіткого розуміння складових персональних даних працівника і видів інформації про особу. Законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, котрі є персональними даними. Задля можливості застосування положень Закону України «Про захист персональних даних» до різноманітних ситуацій, зокрема, що виникають при обробці персональних даних, отриманих у процесі відеоспостереження та використання інших форм моніторингу, необхідно внести відповідні доповнення до Кодексу законів про працю України. Крім того, сьогодні відсутнє належне нормативно-правове регулювання порядку та механізмів проведення перевірок приміщень підприємств, де обробляються персональні дані. Таким чином, представники уповноваженого органу мають право безперешкодно потрапляти до будь-якого приміщення, де обробляються персональні дані (тобто практично до кожного офісу та підприємства), що є рівнозначним праву на проведення обшуку, котре до сьогодні мали лише правоохоронні органи. Підприємство має визначити коло працівників, які працюють з персональними даними (бухгалтерія, відділ кадрів, директор, його заступники, юрисконсульт, адміністратор системи тощо) та які підписують зобов'язання про нерозголошення. Іншим проблемним моментом, що потребує надійної системи захисту персональних даних у процесі їх обробки, є розміщення цих даних в мережі Інтернет. Оскільки персональні дані є або можуть бути об'єктом використання в автоматизованій системі обробки, люди, користуючись мережею Інтернет, залишають там велику кількість своїх даних. І, що головне, використання даних нічим не обмежене і не врегульоване, тобто фактично такі дані залишаються незахищеними. Згадані бази даних постійно вдосконалюються, уніфікуються і щораз більше стосуються приватного життя людини [11]. Щоб захистити свої персональні дані від протиправних посягань, особа може використовувати будь-які не заборонені законом засоби. Зокрема, у випадку незаконної обробки персональних даних та втручання в особисте життя особи суб'єкт персональних даних вправі звернутися до володільця та/або розпорядника персональних даних із вмотивованою вимогою: заборонити таку обробку; внести зміни до власних персональних даних (у випадку їхньої недостовірності); вимагати їх видалення (знищення). Водночас для підвищення захищеності персональних даних працівників мають застосовувати заходи і самі роботодавці [12].

Висновки. Завдяки поширенню технологій спостереження та інтеграції їх у виробництво масштаби спостереження за людиною на робочому місці постійно розширюються та вдосконалюються його форми. Розвиток технологій стеження посилив конфлікт інтересів між роботодавцями та працівниками. Права роботодавців на управління, підпорядкованість працівників і раціональне використання персональної інформації створили багато перешкод для захисту працівниками власних законних інтересів і особистої інформації. Захист особистої інформації працівників можна посилити шляхом прийняття спеціальних законів у сфері праці та захисту персональної інформації. Вважаємо за доцільне доповнити законодавство такими нормами:

1) роботодавець повинен завчасно повідомити працівника про нагляд за робочим місцем у письмовій або електронній формі, а також надати працівникам достатньо часу для заперечень;

2) у повідомленні має бути зазначено зміст, вид відеоспостереження, режим і тривалість зберігання, особу, яка обробляє і зберігає інформацію, та її контактні дані;

3) працівник має право доступу до інформації про нього, що була зібрана в процесі моніторингу;

4) у випадку несанкціонованого витіку персональних даних працівника, що зберігаються роботодавцем, останній повинен якомога швидше повідомити співробітників про це і вжити заходів для нівелювання можливих негативних наслідків.

Список використаних джерел

1. Perna M. C. Why 78% Of Employers Are Sacrificing Employee Trust By Spying On Them. *Forbes*. URL: https://www.forbes.com/sites/markcperna/2022/03/15/why-78-of-employers-are-sacrificing-employee-trust-by-spying-on-them/?sh=6a09ffa91659.

2. Про захист персональних даних : Закон України від 01.06.2010. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

3. Деякі питання практичного застосування Закону України «Про захист персональних даних» : роз'яснення Міністерства юстиції України від 21.12.2011. URL: https://zakon.rada.gov.ua/laws/show/n0076323-11#Text.

4. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України : рішення Конституційного Суду України від 20.01.2012 № 2-рп/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text.

5. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : Директива 95/46/ЄС Європейського парламенту і Ради від 24.10.1995. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text.

6. Конституція України від 28.06.1996. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

7. Ярошенко О. М. Проект Трудового кодексу України (№ 1658 від 27.12.2014 р.) – кодифікований акт чи закон про працю. *Розвиток трудового права і права соціального забезпечення: теорія і практика : тези доп. та наук. повідомл. учасників VIII Міжнародної науково-практ. конф.* (м. Харків, 5 жовт. 2018 р.) ; за ред. О. М. Ярошенка. Харків : ФОП Панов А. Н, 2018. С. 18–24.

8. Чернобай А. М. Поняття персональних даних працівника. *Актуальні проблеми держави і права : зб. наук. праць.* Одеса : Юрид. л-ра, 2004. Вип. 22. С. 827–833.

9. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) : Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

10. Eastern and Northern Europe: The Law on Hidden Video Surveillance of Workers. *Ius Laboris.* URL: https://iuslaboris.com/insights/eastern-and-northern-europe-the-law-on-hidden-video-surveillance-of-workers/.

11. Щербатюк М. Особливості захисту персональних даних в Інтернеті. *Ukrainian internet association.* URL: https://inau.ua/document/osoblyvosti-zakhystu-personalnykh-danykh-v-interneti.

12. Забезпечення захисту персональних даних співробітників підприємств у цифровій економіці з використанням технології блокчейн : наукова робота. *Save Data21.* URL: https://www.hneu.edu.ua/wp-content/uploads/2021/04/66.Save-Data21.pdf.

Надійшла до редакції 10.05.2023

References

1. Perna, M. C. Why 78% Of Employers Are Sacrificing Employee Trust By Spying On Them. *Forbes.* URL: https://www.forbes.com/sites/markcperna/2022/03/15/why-78-of-employers-are-sacrificing-employee-trust-by-spying-on-them/?sh=6a09ffa91659.

2. Pro zakhyst personalnykh danykh [About the protection of personal data] : Zakon Ukrainy vid 01.06.2010. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text. [in Ukr.].

3. Deiaki pytannia praktychnoho zastosuvannia Zakonu Ukrainy «Pro zakhyst personalnykh danykh» [Some issues of practical application of the Law of Ukraine «On Personal Data Protection»] : roziasnennia Ministerstva yustytsii Ukrainy vid 21.12.2011. URL: https://zakon.rada.gov.ua/laws/show/n0076323-11#Text. [in Ukr.].

4. Rishennia Konstytutsiinoho Sudu Ukrainy u spravi za konstytutsiinym podanniam Zhashkivskoi raionnoi rady Cherkaskoi oblasti shchodo ofitsiinoho tlumachennia polozhen chastyn pershoi, druhoi statti 32, chastyn druhoi, tretoi statti 34 Konstytutsii Ukrainy [The Decision of the Constitutional Court of Ukraine in the case of the constitutional submission of the Zhashkiv District Council of the Cherkasy Region regarding the official interpretation of the provisions of the first and second parts of Article 32 and the second and third parts of Article 34 of the Constitution of Ukraine] : rishennia Konstytutsiinoho Sudu Ukrainy vid 20.01.2012 № 2-rp/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text. [in Ukr.].

5. Pro zakhyst fizychnykh osib pry obrobtsi personalnykh danykh i pro vilne peremishchennia takykh danykh [On the protection of natural persons during the processing of personal data and on the free movement of such data] : Dyrektyva 95/46/IeS Yevropeiskoho parlamentu i Rady vid 24.10.1995. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text. [in Ukr.].

6. Konstytutsiia Ukrainy [Constitution of Ukraine] vid 28.06.1996. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80. [in Ukr.].

7. Iaroshenko, O. M. (2018) Proekt Trudovoho kodeksu Ukrainy (№ 1658 vid 27.12.2014 r.) – kodyfikovanyi akt chy zakon pro pratsiu [Draft Labor Code of Ukraine (№ 1658 dated 27.12.2014) – a codified act or law on labor]. *Rozvytok trudovoho prava i prava sotsialnoho zabezpechennia: teoriia i praktyka : tezy dop. ta nauk. povidoml. uchasnykiv VIII Mizhnarodnoi naukovo-prakt. konf.* (m. Kharkiv, 5 zhovt. 2018 r.) ; za red. O. M. Yaroshenka. Kharkiv : FOP Panov A.N. pp. 18–24. [in Ukr.].

8. Chernobai, A. M. (2004) Poniattia personalnykh danykh pratsivnyka [The concept of employee personal data]. *Aktualni problemy derzhavy i prava : zb. nauk. prats.* Odesa : Yuryd. l-ra. Issue

22. pp. 827–833. [in Ukr.].

9. Pro zakhyst fizychnykh osib u zviazku z opratsiuvanniam personalnykh danykh i pro vilnyi rukh takykh danykh, ta pro skasuvannia Dyrektyvy 95/46/IeS (Zahalnyi rehlament pro zakhyst danykh) [On the protection of natural persons in connection with the processing of personal data and on the free movement of such data, and on the repeal of Directive 95/46/EU (General Data Protection Regulation)] : Rehlament Yevropeiskoho Parlamentu i Rady (IeS) 2016/679 vid 27.04.2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text. [in Ukr.].

10. Eastern and Northern Europe: The Law on Hidden Video Surveillance of Workers. *Ius Laboris.* URL: https://iuslaboris.com/insights/eastern-and-northern-europe-the-law-on-hidden-video-surveillance-of-workers/.

11. Shcherbatiuk, M. Osoblyvosti zakhystu personalnykh danykh v Interneti [Peculiarities of personal data protection on the Internet]. *Ukrainian internet association.* URL: https://inau.ua/document/osoblyvosti-zakhystu-personalnykh-danykh-v-interneti. [in Ukr.].

12. Zabezpechennia zakhystu personalnykh danykh spivrobitnykiv pidpryiemstv u tsyfrovii ekonomitsi z vykorystanniam tekhnolohii blokchein [Ensuring the protection of personal data of employees of enterprises in the digital economy using blockchain technology] : naukova robota. *Save Data21.* URL: https://www.hneu.edu.ua/wp-content/uploads/2021/04/66.Save-Data21.pdf. [in Ukr.].

ABSTRACT

Hanna Spitsyna, Svitlana Gutsu. Protection of personal employees' data obtained in the process of video surveillance in the workplace. The state of legal regulation of protection of personal employees' data collected in the course of monitoring and video surveillance at the workplace has been studied. It is established that national labour legislation does not have special rules on the specifics of regulation of this issue, but European countries have quite significant developments and a regulatory framework in the field of regulation of such methods of working with personal information.

The authors have proposed to supplement national legislation by defining the rules, grounds and time limits for employer monitoring and video surveillance in the workplace, namly: 1) the employer must inform the employee in advance about the supervision of the workplace in written or electronic form, as well as give employees enough time for objections; 2) the message must specify the content, type of video surveillance, mode and duration of storage, the person who processes and stores the information, and their contact details; 3) the employee has the right to access information about him/her that was collected during the monitoring process; 4) in case of unauthorized leakage of the employee's personal data stored by the employer, the latter must inform the employees about this as soon as possible and take measures to eliminate possible negative consequences.

This will help protect the interests of the parties to labour relations and facilitate the implementation of legislation in the field of personal data protection.

Keywords: *personal information, workplace surveillance, processing of employee personal data, personal data of employees, information, information protection, labour relations, employee, employer, employment contract.*

УДК 342.92: 342.7
DOI: 10.31733/2078-3566-2023-2-178-185

Оксана СТРЕЛЬЧЕНКО©
доктор юридичних наук, професор
(Національна академія внутрішніх справ,
м. Київ, Україна)

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ІНСТИТУТУ АДМІНІСТРАТИВНОЇ ВІДПОВІДАЛЬНОСТІ У ПАРАДИГМІ АДМІНІСТРАТИВНОГО ПРАВА

Охарактеризовано концептуальні засади функціонування адміністративної відповідальності у сучасній доктрині адміністративного права, котра має тривалу історію свого впровадження та трансформації. Незважаючи на усі зміни, шо відбуваються у суспільстві, адміністративна відповідальність є невідривною частиною юридичної відповідальності, котра виявляється у відповідному ставленні осіб до виконання своїх обов'язків, а також у

© О. Стрельченко, 2022
ORCID iD: https://orcid.org/0000-0001-5965-9764
strel1977@ukr.net