УДК 349.2:[342.721:004.056.5]
DOI https://doi.org/10.24144/2307-3322.2022.75.3.8

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ МОНІТОРИНГУ РОБОТОДАВЦЯМИ ВИКОРИСТАННЯ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ, ІНТЕРНЕТ-РЕСУРСІВ ТА КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ ПРАЦІВНИКАМИ У СПОЛУЧЕНИХ ШТАТАХ АМЕРИКИ

Луценко О.Є.,
кандидат юридичних наук, доцент кафедри трудового права
Національного юридичного університету імені Ярослава Мудрого
o.ye.lutsenko@nlu.edu.ua
https://orcid.org/0000-0001-9357-8546
Scopus Author ID: 57194875083

Луценко О.Є. Правове забезпечення моніторингу роботодавцями використання корпоративної електронної пошти, інтернет-ресурсів та комп'ютерних технологій працівниками у Сполучених Штатах Америки.

У статті висвітлюються питання захисту персональних даних працівників, проблеми моніторингу роботодавцями використання корпоративних електронних пошт, бізнес-акаунтів, комп'ютерів та інших дивайсів роботодавця.

Авторка справедливо зауважує, що натепер майже будь-яке програмне забезпечення дозволяє здійснювати комп'ютерний моніторинг та стежити за робочим місцем навіть без обізнаності про це співробітників, а чинне законодавство не покладає на роботодавців обов'язок повідомляти співробітників перед впровадженням такого програмного забезпечення для моніторингу. Проте у багатьох державах таке законодавство існує та вироблена судова практика щодо захисту прав працівників у випадку

У США поширена практика роботодавців, які контролюють електронну пошту чи використання Інтернету без попередження, що загрожує основним правам американських робітників. У США компанії висувають багато причин для спостереження за використанням корпоративної пошти чи Інтернету, зокрема: а) запобігання неправильному (не за призначенням) використанню корпоративної пошти, втрата ефективності роботи співробітників в Інтернеті; б) мережева політика компанії; в) запобігання судовим позовам про дискримінацію, переслідування чи інші правопорушення в Інтернеті; г) запобігання несанкціонованій передачі інтелектуальної власності та уникнення здійснення незаконних копій захищених авторським правом матеріалів працівниками; д) збереження документації компанії; е) запобігання незаконному привласненню особистої інформації, потенційному спаму або «вірусним програмам»; є) захист активів компанії, в тому числі інтелектуальної власності та бізнес-планів

Авторка також аналізує проблему щодо того, які кроки робить компанія, щоб обмежити використання корпоративних комп'ютерів для особистого використання працівниками.

Усе більше американських компаній контролюють електронну пошту та Інтернет-комунікації своїх працівників, щоб зменшити ризик вчинення правопорушень працівниками. Комп'ютерні системи, надані роботодавцем, але використані працівниками не за призначенням, можуть призвести до претензій щодо дискримінації або сексуальних домагань чи до поширення образливих електронних листів чи Інтернет-графіки, повідомлень, наклепів, а також до порушення авторських прав, шахрайства, чи навіть стати підставою для позовів, пов'язаних із неправомірною поведінкою працівників. Окрім цього, жарти електронною поштою або грубі заставки також можуть наражати роботодавця на позов про харазмент.

Ключові слова: інформація, захист інформації, конфіденційна інформація, персональні дані працівників, діджиталізація, трудові правовідносини, працівник, роботодавець.

Lutsenko O. Legal security for employer monitoring of employee use of corporate email, internet resources, and computer technology in the United States of America.

The article covers issues of the protection of employees' personal data, and problems of monitoring by employers of the use of corporate e-mails, business accounts, computers and other devices of the employer.

The author rightly notes that now almost any software allows for computer monitoring and monitoring of the workplace even without the knowledge of employees, and the current legislation does not oblige employers to notify employees before implementing such monitoring software. However, in many states, such legislation exists and case law has been developed to protect the rights of employees in the event

In the US, it is common practice for employers to monitor e-mail or Internet use without warning, threatening the basic rights of American workers. In the US, companies put forward many reasons for monitoring the use of corporate e-mail or the Internet, in particular: a) prevention of improper (non-intended) use of corporate e-mail, loss of efficiency of employees' work on the Internet; b) network policy of the company; c) prevention of lawsuits about discrimination, harassment or other offenses on the Internet; d) prevention of unauthorized transfer of intellectual property and avoidance of illegal copies of copyrighted materials by employees; e) preservation of company documentation; e) prevention of illegal appropriation of personal information, potential spam or "virus programs"; g) protection of the company's assets, including intellectual property and business plans

The author also analyzes the problem of what steps the company takes to limit the use of corporate computers for personal use by employees.

A growing number of American companies are monitoring their employees' e-mail and Internet communications to reduce the risk of employee wrongdoing. Computer systems provided by an employer but misused by employees may lead to claims of discrimination or sexual harassment or to the distribution of offensive e-mail or Internet graphics, messages, defamation, copyright infringement, fraud, or even become the basis for lawsuits related to employee misconduct. In addition, e-mail jokes or crude screenplays can also expose an employer to a harassment claim.

Key words: information, information protection, confidential information, personal data of employees, digitization, labour relations, employee, employer.

Постановка проблеми. Нині неможливо уявити кожне робоче місце без використання електронної пошти, Інтернету, браузерів та веб-порталів. Працівники «виходять» в Інтернет через їхні мобільні телефони, пейджери, планшети чи комп'ютери. Тому кіберпростір стає все більшою і більшою частиною сучасного робочого місця, позаяк це те місце, де компанії розміщують веб-сайти, виконують замовлення, надають професійні послуги та спілкуються в електронному вигляді з дочірніми компаніями по всьому світу. Компанії збільшили їх продуктивність і ефективність завдяки інформаційним технологіям, але у той же час зловживання Інтернетом змусили компанії контролювати електронні комунікації та захищати свої права.

Наразі підхід до електронного моніторингу залишив американських працівників без реальних засобів захисту від нав'язливого електронного контролю. У світі зловмисних хакерів, недбалих співробітників і широкого поширення корпоративного шпигунства, компаніям вкрай важливо захистити їхні інформаційні активи. Тому відсутність моніторингу електронної пошти співробітників або використання Інтернету наражає бізнес на катастрофічні збитки через репутаційні, юридичні та бізнес-ризики, що виникають внаслідок «витоку» комерційної таємниці, бізнес-планів та іншої конфіденційної інформації, зокрема і персональних даних працівників.

Компанії США стають більш конкурентоспроможними в глобальній економіці завдяки гармонізації робочих місць та моніторингу режиму конфіденційності інформації про торгових партнерів та співробітників. Однак такий моніторинг має належним чином збалансовувати *потребу роботодавця* у моніторингу та *право працівника на конфіденційність*, коли йдеться про чутливу інформацію, особистих фінансів та відносин чи іншої приватної інформації, яка не пов'язана з робочим місцем, але може стати відомою роботодавцеві під час контролю за працівниками.

Стан опрацювання проблематики. Питання захисту персональних даних працівника мало досліджуються українськими вченими. Наразі можна виокремити лише декількох вчених-трудовиків, які цікавляться цією проблематикою, як-от: А.В. Авраменко [1], І.В. Лагутіна [2], Г.І. Чанишева, Р.І. Чанишев [3], А.М. Чернобай [4]. Хоча й науковці недостатньо вдаються до дослідження питань захисту персональних даних працівників, однак на практиці все більше проблем виникає саме з формуванням правового регулювання механізму захисту персональних даних працівників та моніторингу робото-

давцем використання корпоративної пошти для особистих потреб, поширення інформації через Інтернет тощо. Відтак, дослідження зарубіжного досвіду може стати у нагоді для вироблення найкращих ідей для удосконалення правового регулювання захисту персональних даних працівників в Україні.

Метою статті є аналіз правового регулювання та практики забезпечення захисту персональних даних працівників у Сполучених Штатах Америки.

Виклад основного матеріалу. Ще десять років тому дотримання вимог конфіденційності в США було відносно простою справою для американських компаній, адже закони про конфіденційність використовувалися лише за деякими сферами і зачіпали обмежені категорії підприємств. Крім того, міжнародна передача даних не була критичною для багатьох підприємств, тому не було потреби розглядати вимоги, які можуть висувати європейські компанії, а Інтернет-використання тільки зароджувалося [5, с. 18]. Однак наразі на робочих місцях в США відбуваються суттєві зміни, тому конфіденційність на робочому місці стала питанням суттєвих наслідків, особливо тому, що американські робітники стають жертвами шпигунства електронної пошти, яка залишилася без жодного захисту. Очікується, що продажі програмного забезпечення для електронного моніторингу зростуть майже в п'ять разів із 139 мільйонів доларів США до 662 мільйонів доларів США [6, с. 22]. Опитування роботодавців підтвердило, що 70% роботодавців (які приймали участь в опитуванні) запровадили письмову політику контролю електронної пошти, яка регулює використання та вміст корпоративної електронної пошти, а 74% контролюють вихідну та вхідну кореспонденцію співробітників, тоді як 60% стежать за з'єднанням співробітників з Інтернетом [7, с. 255].

Натепер майже будь-яке програмне забезпечення дозволяє здійснювати комп'ютерний моніторинг та стежити за робочим місцем навіть без обізнаності про це співробітників, а чинне законодавство не покладає на роботодавців обов'язок повідомляти співробітників перед впровадженням такого програмного забезпечення для моніторингу.

Кожна друга компанія США не має внутрішньої політики, яка вимагає, щоб їх працівники надали згоду на електронний моніторинг або підтвердження їх моніторингу на робочому місці [8]. Саме тому в США поширена практика роботодавців, які контролюють електронну пошту чи використання Інтернету без попередження, що загрожує основним правам американських робітників. Такий підхід пов'язаний з тим, що в США сформувався підхід, що поширеною є помилка, що «електронна пошта є такою ж приватною та конфіденційною, як і спілкування через поштову службу... Більшість систем електронної пошти, голосової пошти та комп'ютерів не є приватною та конфіденційною [9, с. 123]. Відтак, багато зарубіжних вчених наголошують, що у цьому контексті США та Європа мають суперечливі концепції конфіденційності та захисту персональної інформації працівників. Тоді як Європа має базовий набір правового захисту, то в США його не існує [10, с. 314].

Режим права власності США створив такий механізм обробки персональних даних працівників, що «так як роботодавці володіють робочими інструментами, вони можуть ініціювати моніторинг за їх особистим бажанням» [11, с. 487]. Такі міркування лежать в основі підходу прав власності:1) співробітники не мають права на конфіденційність під час використання корпоративної електронної пошти/Інтернету; 2) право власності роботодавця на ці робочі інструменти дає їй право на контроль їх використання будь-яким способом, який вони вважають за потрібним» [11, с. 499].

У США компанії висувають багато причин для спостереження за використанням корпоративної пошти чи Інтернету, зокрема: а) запобігання неправильному (не за призначенням) використанню корпоративної пошти, втрата ефективності роботи співробітників в Інтернеті; б) мережева політика компанії; в) запобігання судовим позовам про дискримінацію, переслідування чи інші правопорушення в Інтернеті; г) запобігання несанкціонованій передачі інтелектуальної власності та уникнення здійснення незаконних копій захищених авторським правом матеріалів працівниками; д) збереження документації компанії; е) запобігання незаконному привласненню особистої інформації, потенційному спаму або «вірусним програмам»; є) захист активів компанії, в тому числі інтелектуальної власності та бізнес-планів [12].

Існує також проблема щодо того, які кроки робить компанія, щоб обмежити використання корпоративних комп'ютерів для особистого використання працівниками. Так, дослідження використання Інтернету на робочому місці показало, що майже десятка найбільш відвідуваних сайтів працівниками в робочий час – це певні інвестиційні сайти, інтернет-магазини та сайти особистих інтересів. Співробітники також можуть використовувати електронну пошту, щоб запитувати певну інформацію або передавати конфіденційні бізнес-плани конкурентам. Окрім цього, можуть спровокувати загрозу створення ворожого робочого середовища. Однак використання ліцензійного програмного забезпе-

чення надає роботодавцю право моніторингу його працівників, що полягають у захисті його інтелектуальної власності та активів, щоб уникнути порушення прав інтелектуальної власності як його особистих, так й інших осіб [12, с. 837]. Відтак, все більше американських компаній контролюють електронну пошту та Інтернет-комунікації своїх працівників, щоб зменшити ризик вчинення правопорушень працівниками. Комп'ютерні системи, надані роботодавцем, але використані працівниками не за призначенням, можуть призвести до претензій щодо дискримінації або сексуальних домагань чи до поширення образливих електронних листів чи Інтернет-графіки, повідомлень, наклепів, а також до порушення авторських прав, шахрайства, чи навіть стати підставою для позовів, пов'язаних із неправомірною поведінкою працівників. Окрім цього, жарти електронною поштою або грубі заставки також можуть наражати роботодавця на позов про харазмент.

Окрім заяв про домагання, найбільша небезпека – це ймовірність того, що співробітники або колишні співробітники скористаються комп'ютерами компанії для розголошення комерційної таємниці. Навіть колишній працівник може передати паролі або інші засоби автентифікації, що надає можливість завантажувати файли та записи одним натисканням кнопки, адже електронна пошта надає користувачам комп'ютерів засоби для передачі файлів, даних, зображень і навіть відео миттєво [13]. Ці незаконні передачі можуть поставити під загрозу торгові марки, патенти, авторські права та комерційні таємниці, важливі для виконання бізнес-планів. А компанія, яка не стежить за схоронністю своєї комерційної таємниці, може втратити найбільш цінні активи. Після розкриття, конфіденційна інформація втрачає свій статус комерційної таємниці, яка визначається як будь-яка інформація, включаючи формули, шаблони, компіляції, програми, пристрої, методи, техніку або процеси, що має самостійне економічне значення [14].

Значний ризик ще полягає в тому, що компанія може зазнати негативного впливу через завантаження його співробітниками неавторизованих копій захищених авторським правом програмного забезпечення, музики чи розваг на офісних комп'ютерах. Такий одноранговий файл програми спільного доступу дозволить користувачам Інтернету підключатися безпосередньо один до одного, до комп'ютерів і обмінюватися файлами без розбору, порушуючи авторські права та права на товарний знак.

Важливо зауважити, що розробники Конституції США, звісно, не могли передбачити ступеня розвитку технологій та нові технології можуть порушити конфіденційність усіх американців. Тому в Конституції США конфіденційність прямо не розглядається як фундаментальне право [15]. Лише 4-та поправка до Конституції США захищає конфіденційність, обмежуючи поліцейські обшуки та арешти, але конфіденційність з точки зору автономії не згадується в тексті Конституції [16].

На жаль, працівники США не мають конституційних засобів правового захисту проти приватного моніторингу роботодавцем, навіть якщо такий моніторинг здійснюється дискримінаційно, без повідомлення. Натомість працівники державного сектора мають деякі гарантії щодо конституційного захисту від зловживань такого моніторингу, оскільки на роботодавців у державному секторі поширюються конституційні обмеження, наприклад, право на обґрунтовані обшуки та виїмки [17]. За конкретними справами, американські суди постановили, що працівник державного сектору має право на конфіденційність надісланих або отриманих електронних листів чи повідомлень через Інтернет.

Однак 4-та поправка до Конституції США захищає держслужбовця на робочому місці, лише якщо він довів як суб'єктивну, так і об'єктивну сторони порушення приватності на місці обшуку. Так, у справі *Leventhal v. Knapek* [18], розслідування Департаменту транспорту виявило докази неправильного використання комп'ютера працівником. Суд визнав, що працівник розумно сподівався на конфіденційність, але дійшов висновку, що слідчий обшук не порушив його прав за Четвертою поправкою, оскільки інтереси роботодавця щодо конфіденційності були переважені інтересами законної мети проведення обшуку. Четверта поправка не застосовується до обшуку, якщо не порушується державне втручання та розумне очікування позивача щодо конфіденційності, що є юридично захищеним інтересом. Суд *Knapek* визнав правомірним слідчий обшук, оскільки він був розумним за обсягом і досяг законної мети роботодавця щодо пошуку доказів неправомірних дій працівника. Відтак, у США саме суди врівноважують принцип конфіденційності та зацікавленість роботодавця в державному секторі, але вони не застосовують таке балансування до робочих місць приватного сектору.

У США право на приватність не лише не було включено до Конституції, але й не розвивалося аж до XX ст. Однак у деяких штатах регламентовано певний ступінь конституційного захисту інтересів працівників, що ґрунтуються на приватності. Так, штат *Delaware* прийняв статут, який вимагає від роботодавців надавати інформацію співробітникам, перш ніж розпочати контролювати їх електронну пошту або використання Інтернету [19]. Роботодавці дотримуються статуту штату Делавер, надавши

працівникам інформацію про політику або заходи моніторингу шляхом «одноразового попередження» працівника письмово або в електронній формі, яка має бути підтверджена працівником. А ось штат *Connecticut* вимагає від роботодавців сповіщати працівників електронною поштою чи через Інтернет про здійснюваний моніторинг [20]. Ще у 2000 році сенат Каліфорнії прийняв закон, який вимагав від роботодавців отримувати від усіх працівників електронні та паперові копії всіх документів щодо погодження політики електронного моніторингу. Крім того, працівники повинні або підписати, або задекларувати згоду в електронному вигляді, що вони «прочитали, зрозуміли і дали згоду на політику та практику моніторингу з боку роботодавця». Тому таємний моніторинг розглядається як правопорушення. Однак все ж переважна більшість штатів не мають законів чи прецедентного права, які вимагали б від роботодавців повідомляти працівників про встановлення електронного спостереження/моніторингу.

Важливо зауважити, що *Louis Brandeis* та *Samuel Warre*n вперше запропонували нове деліктне право за вторгнення в приватне життя працівників у своїй науковій статті, опублікованій в *Harvard Law Review* ще у 1890 р. [21, с. 383]. На той час поштовхом до написання цієї наукової праці послужило вироблення пропозицій щодо нових засобів захисту від зловживань з боку друкованих ЗМІ. Їх стаття мала суттєвий вплив на визнання на рівні штатів принципу конфіденційності, навіть Верховний суд США спирався на *Louis Brandeis* та *Samuel Warre*n, формулюючи право на приватність працівників, як «право бути залишеним наодинці» [22]. Це нове на той час право стало так би мовити продовженням права на життя, а точніше права насолоджуватися життям без втручання ззовні. Однак лише в 1960 році *William Prosser* сформулював чотири можливих проступки щодо порушення вимог про приватність працівників: (1) втручання в приватний простір; (2) присвоєння чужого нікнейму в Інтернеті; (3) висвітлення фактів під хибним кутом; та (4) публікація приватних фактів [23, с. 383]. Більшість юрисдикцій штатів визнали ці чотири правопорушення, однак за ці правопорушення ще не відбулося розширення застосування покарання та запобігання необґрунтованому нагляду за працівниками на робочому місці.

Із самого початку застосування електронної пошти, було визнано, що вона так би мовити є гібридним середовищем з атрибутами кількох різних засобів зв'язку. Проблема полягала в тому, щоб визначити – чи є електронні листи функціонально еквівалентні телеграфу, листівкам, телефонним дзвінкам або радіозв'язку. Суди штатів визнали, що працівники мають право на конфіденційність, користуючись звичайною поштою (друкованою). Приміром, Суд *Jackson* виокремив «звичайну пошту» призначену зберігати без огляду, такі файли як-от: листи, запечатані пакунки, газети, брошури та листівки, які можна було оглянути чи навіть читати поштовими інспекторами, не відкриваючи. Суд зазначив, що якщо інспектор відкрив закритий лист, то принцип конфіденційності було порушено, але його не було порушено в читанні відкритої пошти [24].

Matthew W. Finkin справедливо стверджує, що відкривати пошту співробітника, позначену як «особиста» порушує конфіденційність, однак навіть, відкриваючи пошту лише для того, щоб перевірити, чи вона приватна чи бізнес-пошта, теж є порушенням конфіденційності. Так, у справі *Vernars v. Young*, керівник відкрив пошту з позначкою «особиста», адресовану конкретному працівнику. Суд вирішив, що працівник мав право на конфіденційність його особистої пошти, адресованої йому та позначеної як особиста, навіть якщо така пошта була доставлена в офіс корпорації [25]. На жаль, натепер жоден суд США не поширив цю саму логіку на розрізнення між особистим та діловим спілкуванням електронною поштою.

В американській культурі найбільше занепокоєння викликає вторгнення в приватний простір працівників через спостереження з боку державних органів, а не тільки від моніторингу на робочих місцях у приватному секторі. Після суперечливого рішення про прослуховування телефонних розмов, Конгрес прийняв Федеральний закон про зв'язок (FCA). Розділ 605 FCA забороняє несанкціоноване перехоплення будь-якого повідомлення та оприлюднення чи публікацію його вмісту, змісту, мети, ефекту або значення такого перехопленого повідомлення, якщо відправник не дав згоди. Конгрес розробив спеціальні вказівки щодо перехоплення повідомлень співробітниками правоохоронних органів у Розділі III закону про боротьбу зі злочинністю та Закону про безпечні вулиці 1968 року, який також відомий як Федеральний закон про прослуховування [26].

У 1986 році Конгрес модернізував Федеральний закон про прослуховування телефонних розмов і ввів у дію Закон про електронне спілкування і Закон про конфіденційність комунікацій 1986 року (*Electronic Communications Privacy Act of 1986 (ECPA*) для розширення захисту конфіденційності. Електронна пошта входить до сфери дії ECPA, якщо інформаційні технології мають істотний зв'язок

із міждержавною торгівлею. Розділ I ECPA забороняє «перехоплення» електронних комунікацій, такі як телефонні дзвінки та електронна пошта. Розділ II містить вказівки щодо того, що є незаконним доступом і розголошенням комунікації в електронному сховищі, наприклад, повідомлення залишені голосом. Електронна пошта, як форма електронної комунікації, має також забезпечувати захист конфіденційності. ECPA забороняє лише «перехоплення» електронних засобів комунікацій. «Перехоплення» визначається як «слухове або інше отримання вмісту будь-якого дротового, електронного чи усного повідомлення через використання будь-якого електронного, механічного чи іншого пристрою». Відповідно до Закону про прослуховування телефонних розмов є три види діяльності, які заборонені: (а) перехоплення або намагання перехопити електронні повідомлення, (б) розкриття або намагання розкрити перехоплену інформацію та (в) використання змісту перехопленої інформації.

Отже, роботодавець, який контролює електронну пошту або перехоплює Інтернет-комунікації працівників вважається такими, хто перехоплює електронний зв'язок у розумінні ECPA. У цьому контексті перехоплення має бути навмисним, тобто особа здійснюючи перехоплення, повинна знати або мати підстави знати, що інформація була незаконно перехоплена. Електронні комунікації, включаючи електронну пошту, це всі повідомлення, які не є дротовими або усні повідомлення. Третім сторонам дозволено контролювати трансакційну інформацію електронної пошти, наприклад, хто є відправником і одержувачем, дату й час, а також тематичний заголовок повідомлення. Разом з цим, розділ I ECPA захищає лише вміст повідомлень під час передачі, а от до роботодавця щодо пошуку вже збережених повідомлень електронної пошти співробітника цей розділ не застосовується.

Існує два законодавчих винятки щодо розділу I ECPA, які застосовуються до електронних комунікацій у контексті працевлаштування. По-перше, ECPA дозволяє постачальникам послуг або будь-кому іншому перехоплювати та розкривати електронне повідомлення, де відправник або одержувач повідомлення фактично надав згоду на розкриття, явно або неявно. Згода, як визначено в ECPA, також охоплює неявну згоду, яка у разі моніторингу працівників, може бути досягнута, коли роботодавець попередньо сповіщає своїх працівників про те, що він контролюватиме повідомлення електронною поштою. По-друге, існує «звичайний курс-бізнес», який за певних обставин може дозволити роботодавцеві контролювати електронну пошту своїх співробітників. Зокрема, роботодавець має винятки для виконання «звичайної діяльності», щоб продемонструвати, що: (а) пристрій, який використовується для перехоплення електронної інформації – це «телефонний або телеграфний прилад, обладнання або будь-який його компонент, наданий або встановлений роботодавцем, і (б) цей пристрій використовується роботодавцем у межах звичайного перебігу бізнесу. Однак роботодавцю дозволено лише перехоплювати, щоб визначити характер спілкування. Тому якщо спілкування виявиться особистим, роботодавець повинен припинити подальше перехоплення комунікацій.

У цьому контексті суд по справі *Adams v. City of Battle Creek* відмовився застосувати виняток ECPA «звичайного курсу-бізнесу». У цій справі міська поліція штату таємно стежила і прослуховувала пейджер одного із офіцерів департаменту поліції. Позаяк поліцейський відділ вважав, що його офіцер допомагав торговцям наркотиками. Однак Суд постановив, що ця ситуація не підпадає під виняток «звичайної діяльності», враховуючи те, що офіцер не мав повідомлення про моніторинг. Суд міркував, що «звичайний курс» вимагає, щоб використання було (1) для законної комерційної мети, (2) звичайною справою та (3) з попереднім повідомленням працівника. Суд відхилив аргумент департаменту про те, що у нього були причини стежити за пейджером через загальну заборону департаменту щодо особистого використання цього пристрою. Суд пояснив, що це було постфактум виправдання для перехоплення пейджера, тим паче, що департамент знав, що багато офіцерів використовували пейджери для особистого користування. Тому Суд дійшов висновку, що ситуація не підпадає під жоден із законних винятків, передбачених федеральними законами про прослуховування.

У справі *Arias v. Mutual CentralAlarm Services, Inc.*, колишні співробітники фірми, що надає послуги сигналізації, вимагали грошової компенсації від свого роботодавця за перехоплення телефонних розмов відповідно до федерального закону про прослуховування. Колишні працівники стверджували, що їхній колишній роботодавець незаконно перехоплював приватні телефонні розмови шляхом запису таких розмов на диктофон. Федеральний окружний апеляційний суд підтвердив, що згода лише однієї із сторін не була необхідною та достатньою для прослуховування телефонних розмов. Також суд встановив, що компанія приховано перехоплювала телефонні розмови співробітників, безперервно та цілодобово, записуючи телефонні розмови всіх своїх працівників. Але у цій справі Суд керувався тим, ці дзвінки виникли в ході «звичайної діяльності», оскільки власник мав законні підстави для

своєї підозри, що його працівники не були лояльними. Тому компанія мала законні ділові причини «підтримувати постійний запис усіх вхідних та вихідних телефонних дзвінків». Суд мотивував це тим, що компанія сигналізації була сховищем «надзвичайно чутливої безпекової інформації, включаючи інформацію, яка може полегшити доступ до приміщень їх клієнтів». Відтак, Суд зазначив, що діяльність компанії є настільки широкою, що навіть включала спостереження за розмовами про особисті відносини працівників компанії [12, с. 848-849].

Висновки. Наразі будь-яке програмне забезпечення дозволяє здійснювати комп'ютерний моніторинг та стежити за робочим місцем навіть без обізнаності про це співробітників, а чинне законодавство не покладає на роботодавців обов'язок повідомляти співробітників перед впровадженням програмного забезпечення для моніторингу. У США поширеним є такий механізм обробки персональних даних, що дозволяє роботодавцям як володільцям цими робочими інструментами ініціювати та здійснювати моніторинг лише за їх особистим бажанням.

У США компанії мають багато причин для електронного контролю працівників, зокрема: а) запобігання неправильному (не за призначенням) використанню корпоративної пошти, втрата ефективності роботи співробітників в Інтернеті; б) мережева політика компанії; в) запобігання судовим позовам про дискримінацію, переслідування чи інші правопорушення в Інтернеті; г) запобігання несанкціонованій передачі інтелектуальної власності та уникнення здійснення незаконних копій захищених авторським правом матеріалів працівниками; д) збереження документації компанії; е) запобігання незаконному привласненню особистої інформації, потенційному спаму або «вірусам»; є) захист активів компанії, в тому числі інтелектуальної власності та бізнес-планів.

Все більше американських компаній контролюють електронну пошту та Інтернет-комунікації своїх працівників, щоб зменшити ризик вчинення правопорушень. Комп'ютерні системи, надані роботодавцем, але використані працівниками не за призначенням можуть призвести до претензій щодо дискримінації або сексуальних домагань чи щодо поширення образливих електронних листів чи Інтернет-графіки, повідомлень, наклепів, а також порушення авторських прав, шахрайство, чи навіть стати підставою для позовів, пов'язаних із неправомірною поведінкою працівників.

У більшості штатів у США працівники не мають конституційних засобів правового захисту проти приватного моніторингу роботодавця, навіть якщо він здійснюється дискримінаційно, без повідомлення. Натомість працівники державного сектора мають деякі гарантії щодо конституційного захисту від зловживань моніторингу, оскільки на роботодавців у державному секторі поширюються конституційні обмеження. Лише у деяких штатах регламентовано певний ступінь конституційного захисту інтересів працівників, що ґрунтуються на приватності.

Список використаних джерел:

1. Авраменко А.В. Правове регулювання відносин щодо обігу та захисту персональних даних працівника в трудовому праві України: дис. канд.юрид.наук: 12.00.05. Київ, 2019. 228 с.
2. Лагутіна І.В. Особисті немайнові трудові права працівників у системі трудових прав: монографія. Одеса: Фенікс, 2014. 428 с.
3. Чанишева Г.І., Чанишев Р.І. Право на інформацію за трудовим законодавством України: монографія. Одеса: Фенікс, 2012. 196 с.
4. Чернобай А.М. Правові засоби захисту персональних даних працівника: Дис. …канд. юрид. наук: 12.00.05. Одеса, 2006. 200 с.
5. Lisa J. Sotto & Martin E. Abrams, Needed: A Master Lock for Data, RECORDER, Jan. 21, 2005. 45 p.
6. Robin L. Wakefield, Computer Monitoring and Surveillance: Balancing Privacy with Security, 74 CPA J. 52 (July 1, 2004) (quoting an International Data Corporation study). 50 p.
7. Reginald C. Govan & Freddie Mac, 33rd Annual Institute on Employment Law: Workplace Privacy, 712 PLI/LIT 245, 251 (2004), available at WESTLAW, TP-ALL Library 255 p.
8. Survey: Most Employers Monitor E-mail, Internet Use, SACRAMENTO Bus. J., Oct. 8, 2003, URL: http://www.bizjoumals.com/sacramento/stories/2003/10/06/daily20.html.
9. C. Forbes Sargent, III, Electronic Media and the Workplace: Confidentiality, Privacy and Other Issues, 41 BOSTON BAR J. 6, 6 (May-June 1997). 305 p.
10. Joel R. Reidenberg, E-Commerce and Trans-Atlantic Privacy, 38 Hous. *L. REV.* 717, 718 (2001). P. 314.

11. Karen Eltis, The Emerging American Approach to E-Mail Privacy in the Workplace: Its Influence on Developing Caselaw in Canada and Israel: Should Others Follow Suit? CoMP. LAB. L. & POL'Y J. 487, 499 (2003).
12. Michael L. Rustadt & Sandra R. Paulsson Monitoring employee e-mail and internet usage: avoiding the omniscient electronic sweatshop: insights from Europe. U. PA. Journal Of Labor And Employment Law. Vol. 7:4. P. 829–904, c. 837.
13. United States v. Martin, 228 F.3d 1 (1st Cir. 2000) (affirming criminal conviction of employee who conspired via e-mail to steal trade secrets from a veterinary laboratory); James Garrity and Eoghan Casey, Internet Misuse in the Workplace: A Lawyer's Primer,72 FLA. B. J. 22 (Nov. 1998).
14. UNIF. TRADE SECRETS ACT § 1(4) (2004).
15. MADELEINE SCHACHTER, INFORMATIONAL AND DECISIONAL PRIVACY 8 (2003) ("Constitutional privacy law has evolved largely from textual and inferential construction of the Bill of Rights; in particular, the First, Fourth, Fifth, and Ninth Amendments, as well as the Fourteenth Amendment.").
16. Erwin Chemerinsky, Privacy and the Alaska Constitution: Failing to Fulfill the Promise,20 ALASKA L. REV. 29, 29 (2003) (citations omitted).
17. O'Connor v. Ortega, 480 U.S. 709 (1987) (finding that the strictures of the Fourth Amendment apply to government employers).
18. 266 F.3d 64 (2d Cir. 2001).
19. DEL. CODE ANN. tit. 19, § 705 (2005).
20. DAVID W. QUINTO, THE LAW OF INTERNET DISPUTES § I1.03[A] at 11-59 (2002).
21. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy,4 HARV. L. REv. 193 (1890).
22. Katz v. United States, 389 U.S. 347, 350 & n.6 (1967).
23. William L. Prosser, Privacy, 48 CAL. L. REV. 383 (1960); W. PAGE KEETON ET AL., PROSSER AND KEETON ON TORTS § 11 (5th ed. 1984). 383.
24. Matthew W. Finkin, Employee Privacy, American Values and the Law, 72 CH.-KENT. L. REv. 221, 225 (1996).
25. 539 F.2d 966 (3d Cir. 1976).
26. The Omnibus Crime Control and Safe Streets Act (The Federal Wiretap Act or Title III), Pub. L. No. 90-351, (codified at 18 U.S.C. §§ 2510-2520 (1968)).