DOI 10.69085/PSC2025427

ДОПУСТИМ И НЕОБХОДИМ ЛИ Е КОНТРОЛЪТ С ТЕХНИЧЕСКИ СРЕДСТВА ОТ СТРАНА НА РАБОТОДАТЕЛЯ НАД ПОВЕДЕНИЕТО НА РАБОТНИЦИТЕ И СЛУЖИТЕЛИТЕ, ВКЛЮЧИТЕЛНО В ЕЛЕКТРОННА СРЕДА?

доц. д-р Андрей Александров
Институт за държавата и правото при БАН
Югозападен университет, България

Резюме: *Новите информационни и комуникационни технологии не само позволяват, а и правят неизбежно все повече трудови задължения да се изпълняват онлайн. Показателно в това отношение е и първото по рода си регламентиране в законодателството на ЕС на условията на труд на работещите през платформи (или т.нар. Директива за платформените работници). Тя излиза извън предмета на настоящото изложение, но сама по себе си е безспорно доказателство за значимостта на Интернет комуникацията днес, която само допреди няколко десетилетия изглеждаше като научна фантастика. Огромен брой хора по света, както и у нас, прекарват цялото или почти цялото си работно време пред компютър или друго електронно устройство и общуват с колегите, ръководителите и трети лица преимуществено в електронна среда. Това налага необходимостта от постоянна дискусия за границите на работодателския контрол над поведението на работниците и служителите онлайн. Формулиран още по-общо, този въпрос може да се постави и така: докъде се простира свободата на работодателя да контролира своите служители чрез технически средства?*

Ключови думи: *работодателски контрол, информационни и комуникационни технологии, нарушения на трудовата дисциплина, защита на личните данни.*

IS THE EMPLOYER'S CONTROL BY TECHNICAL MEANS OVER THE EMPLOYEES' BEHAVIOR, INCLUDING IN AN ELECTRONIC ENVIRONMENT ADMISSIBLE AND NECESSARY?

Assoc. Prof. Andrey Aleksandrov, PhD
Institute for the State and the Law – BAS
South-West University, Bulgaria

Abstract: *New information and communication technologies not only allow but also make it inevitable that an increasing number of work duties are performed online. In this respect, the first regulation of its kind in EU legislation on the working conditions of platform workers (or the so-called Platform Workers Directive) is also indicative. Although beyond the scope of this study, it stands as indisputable proof of the importance of Internet communication today – something that only a few decades ago seemed like science fiction. A huge number of people around the world, including in our country, spend all or almost all of their working time in front of a computer or other electronic device, communicating predominantly with colleagues, managers, and third parties in an electronic environment. This situation necessitates an ongoing discussion about the limits of employer control over employee behaviour online. Formulated more generally, this question can also be put as follows: how far does the employer's freedom to control his employees by technical means extend?*

Key words: *employer's control, information and communication technologies, breaches of the labour discipline, personal data protection.*

I. Въведение

Информационните и комуникационните технологии вече са неизменна част от ежедневието както в личен, така и в служебен план, а работата на огромен брой работници и служители е практически невъзможна без използването на компютри, таблети, смартфони и пр. Традиционните форми на кореспонденция в голяма степен се изместват от общуването чрез Интернет, като ежедневно се генерира все по-голям брой електронни съобщения. По принцип тези промени водят до много по-бърз обмен на информацията и предполагат увеличаване на ефективността и производителността на трудовия процес, което ги прави задължителни за адекватната организация на труда при почти всички работодатели. Но те поставят нови въпроси от правно, а и от морално естество, на които действащото законодателство рядко е в състояние да даде своевременен отговор. Затова все повече работодатели се опитват да регулират използването на електронните форми на комуникация от страна на персонала чрез вътрешни актове с цел да гарантират ефективността на работата, спазването на трудовата дисциплина, както и да въведат мерки за информационна сигурност.

Несъмнено пандемията от COVID-19 даде нов тласък на „дигитализирането" на трудовите отношения, защото доведе до лавинообразно нарастване на случаите на полагане на дистанционен труд (надомна работа или работа от разстояние).[1] Същевременно и без нея

[1] Вж. по-подробно Александров, А. Проблеми на трудовите отношения в условията на обявено извънредно положение или обявена извънредна епидемична

тази тенденция щеше да е неизбежна – когато всичко необходимо за изпълнението на служебните задължения в общи линии се свежда до сигурна Интернет връзка, смисълът от пребиваването на едно единствено работно място до голяма степен се загубва. Пространственото отдалечаване между страните по трудовото правоотношение обаче отново ни връща към темата за контрола: как работодателят да се увери, че работникът или служителят изпълнява съвестно служебните си задължения, уплътнява работното си време и спазва установените за предприятието вътрешни правила, ако трудът се полага от десетки или стотици километри разстояние?

Без претенция за изчерпателност, в настоящото изследване ще бъде направен опит да се систематизират някои често възникващи проблеми относно контрола над активността на работниците и служителите с технически способи, вкл. в електронна среда. Подобен анализ предполага да се поставят въпросите за необходимостта и допустимостта на подобен контрол, способите за неговото осъществяване и правната му уредба – доколкото съществува такава на законово ниво и в т.нар. недържавни източници на трудовото право.[2]

II. Способи за работодателски контрол

В световен мащаб се наблюдава устойчива тенденция към увеличаване на използването на технически средства за контрол над активността на персонала. Монтирането на камери за видеонаблюдение вече се възприема едва ли не като правило.[3] Инсталирането на контролиращ софтуер позволява на работодателя да следи дистанционно мониторите на служебните компютри „в реално време", да ограничава достъпа до определени сайтове и пр. От техническа гледна точка филтрирането и пренасочването на входящата и изходящата електронна кореспонденция е елементарно. Така може да се получи достъп до цялата или част от електронната кореспонденция на служителите, селектирана например по тема, подател или полу-

обстановка. С., Спотинов принт (Aleksandrov, A. Problemi na trudovite otnoshenia v usloviyata na obyaveno izvanredno polozhenie ili obyavena izvanredna epidemichna obstanovka. S., Spotinov print), 2022.

[2] Вж. по-подробно Гевренова, Н. Правилникът за вътрешния трудов ред. С., Сиби (Gevrenova, N. Pravilnikat za vatreshnia trudov red. S., Sibi), 2007, 35 – 80.

[3] Вж. също Фети, Н. Видеонаблюдението на работното място, в контекста на защитата на личните данни. – Труд и право (Feti, N. Videonablyudenieto na rabotnoto myasto, v konteksta na zashtitata na lichnite danni. – Trud i pravo), 2018, № 2, 25 – 37.

чател. В някои предприятия се записват и прослушват всички провеждани телефонни разговори. Широка употреба придобиват и биометричните системи за контрол, базирани на различни измерими индивидуални характеристики на физическото лице, като пръстови отпечатъци.

Най-често посочваните от работодателите цели, които ги мотивират да използват такива контролни механизми, се свеждат до необходимостта от осигуряване на ефективни гаранции за изпълнението на задълженията на работниците и служителите по трудовото правоотношение, като спазване и уплътняване на работното време. Както се посочва и в българската трудовоправна доктрина, нарушение на задължението за уплътняване на работното време е налице, когато работникът или служителят през работно време се отдава на други – извънслужебни, занимания: разговори, пазаруване, уреждане на лични въпроси и др. под. Нарушенията от тази група са между най-често срещаните на практика.[4] Видеонаблюдението и системите за биометричен контрол могат да осигурят надеждна информация за точния час на влизане и излизане на всеки служител от сградата на предприятието, следователно от данните, записани от подобна система, лесно може да се установи дали лицето е било на работното си място през цялата продължителност на установеното работно време.

По отношение на работниците и служителите, работещи от разстояние, контролът чрез технически способи на практика е единствената възможна форма на работодателски контрол.[5] С промените в

[4] Мръчков, В. Трудово право. 9 изд. С., Сиби (Mrachkov, V. Trudovo pravo. 9 izd. S., Sibi), 2015, с. 509.

[5] Без съмнение при полагане на труд в работни помещения, осигурени от работодателя, последният може да упражнява ефективен контрол върху спазването на трудовата дисциплина. Съвсем различно е положението с дома, извънградската къща или други места, от които работникът или служителят може да избере да полага труда си. Обикновено става дума за частна собственост на самия работник или служител или трето лице, което може изобщо да не допусне представител на работодателя или контролен орган в сградата или помещението. От тази гледна точка правилото на чл. 107д, т. 2 КТ (в материята на надомната работа), че работникът или служителят е длъжен да осигурява достъп на работодателя и контролните органи до помещението, където е работното място, за проверка, има по-скоро пожелателен характер. Аналогичното правило в материята на работата от разстояние е с далеч по-„плахата“ формулировка: „*Работниците и служителите, които извършват работа от разстояние, нямат право да откажат достъп до работното място без основание за това, в рамките на*

Кодекса на труда от март 2024 г. в разпоредбата на чл. 107л беше добавена нова алинея 6, според която действително отработеното време на работника и служителя, който извършва работа от разстояние, може да се отчита и чрез автоматизирана система за отчитане на работното време. Работодателят е длъжен при поискване да предостави на работника или служителя, който извършва работа от разстояние, достъп до данните в системата за отработеното от него работно време. В § 1, т. 25 от ДР на КТ е дадена легална дефиниция на понятието „Автоматизирана система за отчитане на работното време" – система за автоматично записване и съхранение на информация с цел отчитане на отработеното време на работниците и служителите.

Наблюдението на активността на служителя в Интернет и контролирането на проведените телефонни разговори е от значение за преценката дали работното време е наситено с изпълнение на служебните задължения. Така работодателят може да придобие и информация за качеството на изпълнение на служебните задължения: компетентност на даваните отговори, любезност, удовлетвореност на клиентите и т.н. Същевременно могат да се разкрият и други нарушения на трудовата дисциплина: не са редки случаите, при които именно чрез използването на съвременните информационни и комуникационни технологии се нарушават задълженията за лоялност към работодателя и опазването на поверителни за него сведения. Ето защо някои работодатели се опитват да наложат пълно ограничение над използването на социални мрежи и мрежи за професионални контакти от служителите си, или поне над споделянето на информация за мястото им на работа (Facebook, LinkedIn и пр.).

Контролът чрез наблюдение на служителите се аргументира още и с необходимостта от предотвратяване на други правонарушения (извън нарушенията на трудовата дисциплина), в това число и престъпления. Това е най-честото оправдание за монтирането на видеокамери – превенция и повишаване на разкриваемостта на кражби в търговски обекти например.[6] Контролът над поведението на служителите в онлайн среда често се свързва и с престъпленията в областта на интелектуалната собственост: на служителите се забранява да инсталират и използват на служебните компютри нелицензи-

установеното работно време и/или на уговореното в индивидуалния и/или в колективния трудов договор." – вж. чл. 107к, ал. 8 КТ).

[6] Романова, Ю. Э. Использование видеонаблюдения для контроля за поведением работников (http://www.delo-press.ru/articles.php?n=6772) (Romanova, Yu. E. Ispolyzovanie videonablyudenia dlya kontrolya za povedeniem rabotnikov).

ран софтуер, а нарочни проверки целят да се установи дали така въведената забрана се спазва. Друга възможна цел на осъществяването на наблюдение над персонала в електронна среда е превенцията от заразяването на служебните компютри и мрежи с компютърни вируси. Известно е, че посещаването на Интернет сайтове с порнографско съдържание се свързва с повишен риск от заразяване с компютърни вируси, което е още една основателна причина то да бъде забранено от служебните компютри.

III. Допустимост на използването на техническите способи за контрол над персонала

Безпредметно би било да се обсъжда темата дали контролът над персонала в онлайн среда е възможен – очевидно способите са многобройни и непрекъснато се увеличават. Факт е също, че те масово се използват от работодателите под най-различен претекст. Остава да се потърси отговор на въпроса доколко това е законосъобразно.

- В една група случаи въвеждането на специални технически мерки за контрол представлява нормативно установено задължение за работодателя. Става дума за дейности, регламентирани в специални закони и свързани с повишени рискове, респ. произтичащите от тях изисквания за сигурност. Например видеонаблюдение се осъществява в банки, казина и изобщо в случаите, в които действащото законодателството предвижда въвеждането на специални мерки за осигуряване на сигурността.
- В други случаи въвеждането на специални технически способи за контрол от работодателя е въпрос на преценка по целесъобразност. Ако счита, че е необходимо да оптимизира трудовия процес по този начин, той следва да извърши задълбочена предварителна оценка на тяхното въздействие и степента, в която мерките биха рефлектирали в личната сфера на работниците и служителите.

- **Преценка от гледна точка на защита на личните данни**

Новите технически способи за контрол поначало са свързани със събиране и съхраняване на данни за физическата идентичност на лицата, т.е. чрез тях се обработват лични данни. Разликата между използваните в близкото минало системи за отчитане с перфокарти и системите за биометричен контрол например (освен че съвременните системи са значително по-надеждни) е именно в натрупването на информационни масиви с лични данни. Следователно първото условие, за да се допусне въвеждането на дадена мярка, е законосъобразното обработване на тези данни.

При видеонаблюдението се създават видеозаписи, съдържащи информация, която по смисъла на законодателството за защита на личните данни е способна да разкрие физическата идентичност на лицето, което е записано. Въпросът за защитата на личните данни се поставя и при използването на други съвременни технически мерки за контрол.

Личните данни на работниците и служителите, събирани от работодателите, най-общо служат за целите на администрирането на трудовите правоотношения.[7] Други данни за същите физически лица, каквито могат да се съдържат в личната им кореспонденция например, не могат да се обработват законосъобразно в същия информационен масив. Ако работодателят разрешава или толерира съхраняването на лична информация на служебните комуникационни средства, той ще трябва да третира цялата информация като такава, респ. не следва да осъществява контрол над съдържанието ѝ.

Посочените принципни положения са валидни и при действието ***на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент за защита на личните данни)***, който започна да се прилага от 25 май 2018 г. Той не промени основните принципи в материята, като обработването на минимално количество данни за ясно установени цели. Регламентът запази и концепцията, че за да е законосъобразно обработването на лични данни е необходимо да е налице поне едно от т.нар. „условия за допустимост на обработването“:

- когато субектът на данните е дал съгласие за обработването;
- когато обработването е необходимо за изпълнението на договор, по който субектът на данните е страна или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
- когато обработването е необходимо за спазването на законово задължение на администратора;
- когато обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

[7] Вж. Александров, А. Защита на личните данни на работниците и служителите. С., Труд и право (Aleksandrov, A. Zashtita na lichnite danni na rabotnitsite i sluzhitelite. S., Trud i pravo), 2016.

- когато обработването е необходимо за изпълнението на задача от обществен интерес или при упражняване на официални правомощия на администратора;
- когато обработването е необходимо за целите на легитимните интереси на администратора, освен когато преимущество пред тези интереси имат интересите или правата и основните свободи на субекта.

Промени се обаче относителната „тежест" на съгласието спрямо останалите основания за законосъобразност на обработването. То е твърде „несигурно" основание, от една страна, защото може лесно да бъде опорочено от работодателя, а от друга, защото субектът на данните винаги може да го оттегли.[8] Същевременно е очевидно, че обработването на личните данни на персонала е необходимо за изпълнението на договор, по който субектът на данните е страна – това е трудовият договор. Обработването на такива данни обикновено е и част от нормативно установени задължения на работодателя по трудовото законодателство. Така за съгласието остава ограничено „приложно поле", когато друго основание липсва – напр. при провеждане на психологически тест на кандидати за работа, който не може да се обоснове с никакво законово или договорно задължение.

Казано накратко, що се отнася до съгласието като условие за допустимост на обработването на лични данни на работниците и служителите, към него трябва да се подхожда внимателно. Разбира се, препоръчително е да има съгласие – било обективирано в клауза в трудовия договор, било в нарочна декларация. Това е най-малкото индикация, че работниците и служителите са запознати с целите на обработването и с правата си по действащото законодателство. Работодателят обаче следва да се стреми да обоснове наличието на някое от другите условия за допустимост и да третира съгласието като „допълнителна", а не като „основна" гаранция за законосъобразност на обработването. Ако събирането и обработването на определена категория данни не произтича пряко от закона и се основава единствено на даденото от лицата съгласие, добре е да се помисли дали наистина тази информация е необходима за целите на трудовото правоотношение и ако не е, да се преустанови използването ѝ. Водещ тук е принципът на минимизиране на обработването – обемът на обработваните лични данни трябва да се сведе до минимално необходимото за постигане на заложените цели.

[8] Вж. по-подробно Тошкова – Николова, Д., Н. Фети Защита на личните данни, С., Труд и право (Toshkova – Nikolova, D., N. Feti Zashtita na lichnite danni, S., Trud i pravo), 2019, 105 – 117.

Специално по отношение на видеонаблюдението практиката се ориентира към оправдаването му с легитимните интереси на администратора (охрана на собствеността и сигурността в обектите) и все по-рядко се търси съгласието на заснеманите лица. В по-новата практика на КЗЛД интерес представлява становище с рег. № ПНМД-17-239/2023 г., с което Комисията се произнася относно законосъобразността на видеонаблюдение за целите на оценка на представянето и изпълнението на трудовите задължения на служители във връзка с определянето на допълнително трудово възнаграждение.[9] Становището е в отговор на запитване от „ЛУКОЙЛ – България“ ЕООД, което е в процес на разработване на система, при която, въз основа на предварително определени критерии за изпълнение на компоненти на трудовите задължения, за служителите по обектите да бъдат предоставяни бонуси към трудовите им възнаграждения. Целта на Дружеството, като работодател, е да има обективно наблюдение за представянето на своите служители по обектите, а не да разчита на субективната преценка на регионалните мениджъри, които пряко отговарят и наблюдават работата на бензиностанциите и на служителите, които работят на тези обекти. Именно, за да има обективност при оценяване изпълнението на компонентите на трудовите задължения от тези служители, Дружеството изразява желание да използва наличните системи за видеонаблюдение по обектите.

С оглед гореизложеното, Дружеството моли КЗЛД да изрази становище по следните въпроси:

1. Възможно и законосъобразно ли е използването на видеонаблюдение за оценка на представянето и изпълнението от страна на служителите на обектите на компоненти от трудовите им задължения по предварително определени критерии и с цел заплащане на лицата на допълнителни възнаграждения с променлив характер, без по никакъв начин това да засяга трудовите възнаграждения с постоянен характер?
2. Възможно и законосъобразно ли е в допълнение на горното и със същите цели и при същите критерии да се използват и аудиозаписи?
3. Следва ли работодателят да извърши предварителни действия и какви, тъй щото обработването на лични данни на служителите по посочения начин да се извършва в съответствие с ОРЗД и ЗЗЛД?

[9] Становището е публикувано в Информационния бюлетин на КЗЛД, бр. 1/2024 г. https://cpdp.bg/wp-content/uploads/2024/01/KZLD_Bulletin_1_106_January_2024.pdf

След обстоен правен анализ КЗЛД стига до заключението, че последващото обработване на записите от видеонаблюдението, включващо и звукозапис за целите на оценката на личностното представяне и изпълнението на трудовите задължения на служителите и за нуждите на определяне на допълнителното им трудово възнаграждение, не съответства на изискванията на чл. 6, пар. 4 от Регламент (ЕС) 2016/679 следователно е недопустимо.

- **Преценка от гледна точка на принципа на неприкосновеност на кореспонденцията**

Предварителната преценка относно допустимостта на въвеждането на технически мерки за контрол следва да отчете и дали чрез предвидената мярка не се нарушава друга изрична нормативноустановена забрана. По-конкретно, става дума за тайната на кореспонденцията.

Европейската конвенция за защита правата на човека и основните свободи[10] гарантира правото на защита и зачитане на личния и семеен живот, неприкосновеността на жилището и тайната на кореспонденцията (чл. 8 ЕКПЧ). Съгласно чл. 34, ал. 1 от Конституцията на Република България тайната на кореспонденцията е неприкосновена, а съгласно чл. 34, ал. 2 изключения от това правило се допускат само с разрешение на съдебната власт, когато това се налага за разкриване или предотвратяване на тежки престъпления. Следва да се приеме, че тези правила се отнасят в еднаква степен както за „обикновената“, така и за електронната кореспонденция.

Тук обаче трябва да се отчете един друг аспект на въпроса, като че ли доловен най-ясно в Закона за държавния служител. Той регламентира правото на неприкосновеност на личната кореспонденция и съобщения на държавния служител, като допълва, че кореспонденция и съобщения, адресирани до държавен служител в това му качество, не се считат за лични. Такава е и логиката на много работодатели, застъпващи тезата, че електронната кореспонденция на служителите от „служебния“ им имейл адрес е именно служебна – създава се и се получава за целите на дейността на работодателя и не може да е неприкосновена в смисъла, който се влага в чл. 34 КРБ. Няма принципна разлика между случаите, в които имейл адресът е предназначен за използване само от конкретния служител и включва името му (от типа ivanov@company.com) и мейлите, които се използват от повече служители (като office@company.com).

[10] Европейската конвенция за защита правата на човека и основните свободи е международен договор, приет в рамките на Съвета на Европа. Той е в сила за Република България от 07.09.1992 г. По силата на чл. 5, ал. 4 от Конституцията Конвенцията е част от вътрешното право на страната и нормите ѝ имат предимство пред тези норми на българското право, които им противоречат.

Тяхното създаване и използване е подчинено на служебни цели, затова е нормално да подлежи на контрол от страна на работодателя. Често срещана практика е при отсъствие на съответния служител да се осигури достъп до тази електронна поща на негов заместник, което за пореден път разколебава идеята за „неприкосновеността" на такава кореспонденция.

Следователно въпросът за допустимостта или недопустимостта на контрола над кореспонденцията се свежда до нейния характер: ако тя е лична, вмешателството на работодателя или на всяко друго лице ще е незаконосъобразно. Обратно, ако тя е изцяло служебна, е оправдано да се признае интересът на работодателя от това да я контролира, както контролира и изпълнението на всяко задължение на работника или служителя по трудовото правоотношение. Ако планира да следи кореспонденцията със служебен характер, работодателят следва първо да забрани използването на съответния имейл за лични цели, в противен случай рискува да наруши конституционно-гарантираните права на служителя чрез разкриване на съдържанието на личната му кореспонденция.

В подкрепа на изложеното становище е и предизвикалото оживени дискусии Решение на Европейския съд по правата на човека от 12.01.2016 г. (Bărbulescu v. Romania, 61496/08, Fourth Section), в което съдът постановява, че е допустимо проследяването на кореспонденция с личен характер в Yahoo Messenger, изпратена от служител в работно време. Решението е правнообвързващо за всички държави, ратифицирали Европейската конвенция за правата на човека, сред които е и България. Решаващ аргумент в полза на изразената теза е, че в дружеството е действала изрична забрана за използване на служебните телекомуникационни средства за лични нужди, която служителят виновно е нарушил.

- **Преценка от гледна точка на опазването на личното достойнство на служителя**

Преценката за допустимостта на използваните технически мерки за контрол трябва да засегне и темата за отражението им върху честта и достойнството на контролираните лица. Съгласно чл. 127, ал. 2 КТ работодателят е задължен „да пази достойнството на работника или служителя по време на изпълнение на работата по трудовото правоотношение." Детайлни законови правила в това отношение липсват, поради което въпросът е деликатен. И все пак някои отговори са очевидни. Например видеонаблюдението може да е допустимо по закон и персоналът да е уведомен за него. Това обаче по никакъв начин не легитимира монтирането на камери в помещения за преобличане, са-

нитарни помещения и други подобни, защото би влязло в противоречие с нормите на морала. Поради същата причина недопустимо би било и използването на системи за биометричен контрол, ако функционирането им е от естество да причини неудобство или унижение на контролираното лице.

По отношение на проследяването и контрола над кореспонденцията, както и контрола над посещаваните Интернет сайтове, въпросът за опазването на достойнството на работника или служителя също не е без значение. За повечето служители не би било приемливо посещенията им в Интернет непрекъснато да се следят и могат да възприемат подобни действия като обида и накърняване на личното им достойнство. При липсата на изрична законова уредба по този въпрос следва да се приеме, че ако работодателят има съображения, поради които желае да забрани достъпа до определени страници, няма пречка да го направи. Компютрите са собственост на предприятието и от работодателя зависи какви рестрикции ще наложи на достъпа до Мрежата от тях. При всяко положение, ако не са въведени ограничения, не следва да се упражнява и особено интензивен контрол над активността на служителите като потребители, защото това представлява намеса в личната им сфера. Що се отнася до контрола над кореспонденция и телефонни разговори, той ще е допустим единствено, ако те са с изцяло служебен характер. Ако не са въведени ограничения за воденето и на лична кореспонденция и разговори от служебните комуникационни средства, проследяването и записването им ще е нарушение и на принципа за опазване на достойнството на работника или служителя.

IV. Механизми за въвеждането на технически мерки за контрол

- **По взаимно съгласие на страните**

Няма пречка по взаимно съгласие на страните по трудовото правоотношение да бъде установен механизъм за контрол на достъпа в предприятието, работното време и т.н. Съгласието на работника или служителя по принцип може да оправдае въвеждането и на всякакви други контролни механизми, стига, разбира се, то да е дадено доброволно и информирано и да не става дума за практики, уронващи достойнството на лицето (вж. по-горе относно съгласието като условие за законосъобразност на обработването на лични данни). Няма пречка например в трудов договор със служител от „call център“ да се предвиди, че проведените телефонни разговори ще се записват с цел подобряване на обслужването на клиентите. С встъпването си в такова трудово правоотношение служителят е информиран и е изразил съгласието си разго-

ворите му да бъдат записвани и прослушвани. Дори да няма изрична забрана за това, вероятно би избягвал провеждането на разговори от личен характер.

- **Едностранно от работодателя**

Работодателят организира, ръководи и управлява трудовия процес. Като елемент от работодателската власт нормотворческата власт се изразява в правомощията на работодателя едностранно да създава общи правила за поведение, задължителни за работниците и служителите, които се намират в индивидуални трудови правоотношения с него.[11]

Съгласно чл. 181 КТ работодателят задължително издава Правилник за вътрешния трудов ред, с който урежда организацията на труда съгласно дейността на предприятието. В този или в отделен вътрешен акт могат и е препоръчително да се включат ясни правила за контрола на достъпа в служебните помещения, предвидените мерки за сигурност, използването на служебните комуникационни средства и др. Така предприетите мерки ще бъдат доведени до знанието на работниците и служителите и задължението да се съобразяват с тях ще се превърне в част от трудовата дисциплина.

В Правилника за вътрешния трудов ред може да се предвиди, че достъпът до служебните помещения ще бъде ограничен и служителите ще влизат и излизат от тях с електронна карта чрез система, използваща пръстови отпечатъци, сканиране на ириса и т.н. Разбира се, обработването на събираните биометрични данни е подчинено на специалния режим на законодателство по защита на личните данни.[12] Самото въвеждане на системата за биометричен контрол обаче е въпрос на преценка от страна на работодателя. Дори предвидените

---

[11] Средкова, Кр. Трудово право. Специална част. Дял I. Индивидуално трудово право. С., УИ „Св. Кл. Охридски" (Sredkova, Kr. Trudovo pravo. Spetsialna chast. Dyal I. Individualno trudovo pravo. S., UI „Sv. Kl. Ohridski"), 2011, с. 38.

[12] Съгласно чл. 25и ЗЗЛД работодател или орган по назначаването, в качеството си на администратор на лични данни, приема правила и процедури при:

1. използване на система за докладване на нарушения;
2. ограничения при използване на вътрешнофирмени ресурси;
3. **въвеждане на системи за контрол на достъпа, работното време и трудовата дисциплина.**

Правилата и процедурите съдържат информация относно обхвата, задълженията и методите за прилагането им на практика. С тях се отчитат предметът на дейност на работодателя или органа по назначаването и свързаното с него естество на работата и не може да се ограничават правата на субектите на данните по Регламент (ЕС) 2016/679 и по този закон. Работниците и служителите се уведомяват за приетите правила и процедури.

предварителни консултации с представителите на синдикалните организации в предприятието и с представителите на работниците и служителите по чл. 7, ал. 2 КТ преди утвърждаването на Правилника за вътрешния трудов ред (чл. 181, ал. 2 КТ) не променят характера му на едностранен акт. Становището на синдикалната организация може и да е, че системата за биометричен контрол създава прекомерни затруднения за персонала; че в тази система се инвестират средства, които биха могли да се изразходват за социално-битово и културно обслужване на работниците и служителите; че системата е неефективна и пр. Въпреки това крайното решение е на работодателя, защото той е носител на правото да се разпорежда с материалните ресурси, използвани за дейността на предприятието.

Наред с разпоредбите на Правилника за вътрешния трудов ред, напоследък набира популярност и издаването на други вътрешни правила, регламентиращи нови форми на работодателски контрол над поведението на персонала в електронна среда – Етични кодекси или Вътрешни правила за използване на комуникационните средства. Често те възпроизвеждат принципи, заимствани от т.нар. „нетикет“ (от думите „интернет“ и „етикет“) или „етикет в Мрежата“. Разбира се, не става дума за пълния набор от такива правила, включващи всички норми на етично поведение и общуване между хората в Интернет пространството.[13] Голяма част от тях зависят от конкретната цел на комуникацията, от стила на кореспонденцията, от културата, възпитанието и начина на изразяване на автора на съобщението и пр. Все пак някои основни моменти могат да се приемат за общовалидни и е удачно да бъдат „пренесени“ и във вътрешната нормативна уредба, създавана от работодателя.

В различни вътрешни актове често се съдържат детайлни правила за „онлайн“ поведението на персонала, напр. ограничения за изпращането на файлове над определен размер. Понякога се забранява и записването на такива файлове на служебните компютри. По този начин донякъде се решават проблемите с претоварването на електронната поща, а и със съхраняването на голям обем информация (при това често с неслужебен характер) на компютрите и сървърите. В допълнение към тези правила някои работодатели въвеждат и рестрикции за посещаването на определени сайтове като социални мрежи

[13] Първото и може би най-известно изследване по въпросите на „нетикет“-а е издадено през 1994 г. от Виржиния Ший. Най-общо може да се каже, че основният принцип, на който е изградена цялата концепция, се свежда до правилото: „В Интернет никога не бива да правиш нещо, за което смелостта не би ти стигнала на живо“ (http://www.albion.com/netiquette/).

или сайтове „с неподходящо съдържание“. Възможно е да се въведат и ограничения за сваляне и инсталиране на програми и т.н.

Удачно е също да се въведат правила за унифицирането на формата на електронната кореспонденция, най-малкото защото тя е израз на корпоративна идентичност. В този смисъл често се предвижда имейлите, изпращани от служителите, да са с един и същи шрифт, сигнатурата им да изглежда по един и същи начин и т.н. Въвеждат се забрани както за използването на служебната електронна поща за лични нужди, така и за използването на лична поща за служебна кореспонденция. Ако се допуска например служителят да препраща служебни имейли до личната си електронна поща, за да има достъп до тях от дома си или други места и да е в състояние да отговаря по-бързо на различни запитвания, оферти и др., това не само повишава риска от изтичане на фирмени тайни, но може да създаде и объркване за клиенти или контрагенти на работодателя, които получават отговори на писмата си от различни имейл адреси.

Много работодатели се опитват да вменят на служителите задължение за пълно разделяне между личната и служебната комуникация. Срещат се и опити за регламентиране на някои допустими изключения: напр. при „вътрешна“ кореспонденция между служители, която може да съдържа и лични елементи (като споделяне на снимки от фирмени тържества и др.п.) Подобни правила навлизат в една твърде деликатна сфера, а правният им ефект е съмнителен. При липса на законова уредба по въпроса е изключително трудно да се предвиди възможният изход от евентуален спор, свързан с контрол от страна на работодателя над електронна кореспонденция, съдържаща лична информация. По аналогичен начин стои и въпросът със записването и прослушването на телефонните разговори. Ето защо, ако се стреми да гарантира в максимална степен възможността си да упражнява контрол над съдържанието на комуникацията, провеждана от служебните комуникационни средства, препоръчително е работодателят да забрани изцяло използването ѝ за лични цели. В противен случай той неизбежно рискува да бъде обвинен в неправомерно вмешателство в личната сфера на работниците и служителите, а и на трети лица.

V. Правни последици при установени нарушения

- **Ангажиране на дисциплинарната отговорност на работника или служителя**

За всяко нарушение на трудовата дисциплина, независимо от това по какъв начин е установено, може да бъде наложено дисциплинарно наказание. Работодателят може да узнае за нарушението чрез

придобиването на непосредствени впечатления, от сигнал от други служители или клиенти, а също така и от запис от видеокамери, записани телефонни разговори, проследена кореспонденция и пр. Законът изисква да е събрана възможно най-пълна информация за извършеното нарушение, в това число да са приети писмените или устните обяснения на работника или служителя. Това е най-важното правило в тази фаза от дисциплинарното производство, защото е гаранция за правото на защита на работника или служителя. Затова и когато работодателят не го е изслушал предварително или не е приел писмените му обяснения, съдът отменя дисциплинарното наказание без да разглежда спора по същество (чл. 193, ал. 2 КТ).

Въпреки че теоретично не съществуват пречки по правилата на дисциплинарната отговорност да бъде санкционирано и нарушение на трудовата дисциплина, установено чрез технически средства за контрол, практиката се сблъсква с многобройни затруднения. Например чрез запис от видеокамера може да се установи, че определен служител не изпълнява или изпълнява неточно трудовите си задължения. На тази база работодателят може да изиска писмените му или устни обяснения по случая. Ако служителят отрече да е извършил нарушение, но работодателят счита, че са налице достатъчно доказателства и наложи дисциплинарно наказание, твърде вероятно е да възникне трудов спор. Доказателствената тежест в този спор ще се носи от работодателя, а дори съдът да допусне видео- или аудиозапис като доказателство по делото – могат да възникнат сериозни затруднения при доказването на автентичността му.

В Решение № 136/11.04.2011 г. на ВКС по гр. д. № 602/2010 г., IV г. о., ГК е даден отговор на въпроса има ли доказателствена стойност видеозапис при установяване на нарушение на трудовата дисциплина. ВКС разяснява, че законът не урежда нарочно и отделно веществените доказателства. Всеки предмет може, съобразно връзката, в която се намира със значимия за спора факт, да носи спрямо него ролята на веществено доказателство. Независимо от липсата на изрично посочване на видеоносителите като веществено доказателство, след като съдържащите се в тях данни могат да бъдат интерпретирани по съответния ред, то може да се приеме, че видеозаписът може да бъде използван за целите на доказването в гражданския процес, включително и при установяване на осъществено дисциплинарно нарушение.

Решение № 221/30.07.2014 г. на ВКС по гр. д. № 7639/2013 г., IV г. о., ГК и Решение № 272/03.10.2014 г. на ВКС по гр. д. № 145/2014 г., IV г. о., ГК са постановени по сходни казуси: чрез камери за видеонаблюдение е констатирано, че продавачи са изисквали от клиентите заплащане на стойността на опаковъчните торбички, предадени от работодателя

за безвъзмездно предоставяне на купувачите в магазина, без да отчитат реализираните приходи. Според съда извършеното съставлява дисциплинарно нарушение по чл. 190, ал. 1, т. 4 и т. 5 КТ – злоупотреба с доверието на работодателя и ощетяване на гражданите чрез измама в цената на стоката, за което законосъобразно е наложено дисциплинарно уволнение. Цитираните случаи са и пример за успешно доказване на фактическата обстановка по случая чрез използване на видеозапис.

- **Ангажиране на други видове отговорност**

Към въпроса за възможните правни последици за работника или служителя от нарушения, установени чрез технически средства за контрол, следва да се отнесе и ангажирането на другите видове юридическа отговорност за съответното нарушение. Както беше посочено, една от възможните цели на осъществявания контрол е превенцията срещу извършване на престъпления, напр. срещу интелектуалната собственост. Ако работодателят установи извършването на такова деяние от негов работник или служител, той е длъжен да уведоми компетентните органи за това. Разбира се, така събраният доказателствен материал няма да е годен за целите на наказателното преследване, но в крайна сметка разкриването и доказването на престъплението е от компетентността на органите на досъдебното производство, а не на работодателя.

Интересен е въпросът с ангажирането на имуществената отговорност на работника или служителя за вреди, причинени на работодателя. По принцип и тук важи изложеното по отношение на дисциплинарната отговорност: независимо от начина на установяване на деянието, няма пречка отговорността на нарушителя да бъде ангажирана, стига да са налице всички предпоставки за налагането на този вид отговорност. При евентуален спор обаче работодателят ще се изправи пред същите практически затруднения в доказването на нарушението, от което са произтекли вредите.

VI. Обобщение

Може да се обобщи, че новите технически възможности за наблюдение и контрол над персонала позволяват почти безгранична намеса в личното пространство на работника или служителя. Макар и технически възможен, такъв ефект е неприемлив и то не само поради правни, а и от нравствено-етични съображения.

Разбира се, ако в предприятието са въведени детайлни правила за използването на информационните и комуникационни технологии, нарушаването им ще съставлява основание за налагане на дисципли-

нарни наказания. Но ако по естеството си опитите на работодателя да осъществява контрол представляват намеса в личната сфера на работниците и служителите и/или могат да доведат до разкриването на съдържанието на лична кореспонденция и определена лична информация за контролираните лица, тяхната законосъобразност ще е – меко казано – съмнителна. С цел избягване на възможни спорове и конфликтни ситуации най-разумно е работодателите да не допускат съхраняването на информация от личен характер на служебните компютри и в служебната електронна поща, а служителите да се съобразяват с така въведените ограничения.

Във всички случаи работодателите трябва внимателно да преценяват крайния ефект на всяка контролна мярка преди нейното въвеждане, за да не допуснат тя да накърни честта, достойнството и правото на неприкосновеност на личната сфера на заетите лица. Подобни действия неизбежно ще доведат до социално напрежение и влошаване на работната атмосфера в предприятието, затова – дори първоначално да спомогнат за подобряването на контрола над трудовата дисциплина – в дългосрочен план ще се окажат непродуктивни. Вместо да залагат на постоянно наблюдение и контрол, работодателите следва да инвестират усилията си в повишаване на удовлетвореността на персонала, изграждане на самодисциплина и насърчаване на личната мотивация на всеки работник или служител. Разбира се, това не изключва контрола за възможни злоупотреби, но като допълващ, а не като основен механизъм за обезпечаване на трудовата дисциплина. Когато се въвеждат ограничения (напр. над посещаването на Интернет сайтове от служебните компютри), тези правила следва да са предварително обсъдени със служителите, да са регламентирани ясно във вътрешната нормативна уредба на предприятието и да не надхвърлят необходимото за осигуряване на нормалното протичане на трудовия процес.

От гледна точка на служителите също е препоръчително да се съобразяват и да подхождат отговорно към подобни ограничения. Напълно нормално и осъществимо е да се установят граници между служебния и личен живот, включително и при поведението в електронна среда. Когато е наясно, че кореспонденцията от служебната му поща или телефонните разговори се контролират, всеки работник или служител би предпочел да използва за съобщения и разговори от личен характер собствената си електронна поща или телефон. Посещаването на Интернет сайтове, над които работодателят е наложил ограничения, винаги може да става от персонален компютър в извънработно време и т.н. Съобщения от личен характер следва да

бъдат получавани и изпращани на лична електронна поща; музикални, видеофайлове и др. да се съхраняват на лични носители. Спазването на подобни елементарни правила би гарантирало избягването на конфликтни ситуации, което в крайна сметка е от взаимен интерес и за двете страни по трудовото правоотношение.