РАБОТНА ГРУПА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПО ЧЛЕН 29

17/BG

WP 249

Становище 2/2017 относно обработването на данни на работното място

Прието на 8 юни 2017 г.

Съдържание

1 Резюме

Настоящото становище допълва предходните публикации на работната група по член 29 (наричана по-нататък „РГ29“) *Становище 8/2001 относно обработването на лични данни в контекста на трудово или служебно правоотношение* (WP48)[1] и *Работния документ от 2002 г. относно наблюдението на електронни съобщения на работното място* (WP55)[2]. След публикуването на тези документи бяха възприети редица нови технологии, които позволяват по-систематично обработване на личните данни на служителите на работното място, което поражда значителни предизвикателства във връзка със защитата на данните и неприкосновеността на личния живот.

В настоящото становище се прави нова оценка на баланса между законните интереси на работодателите и разумните очаквания на служителите за неприкосновеността на личния им живот, като се описват рисковете, породени от новите технологии, и се извършва оценка на пропорционалността на редица сценарии, в които те биха могли да се използват.

Макар че становището е насочено най-вече към Директивата за защита на личните данни, в него се обръща внимание и на допълнителните задължения за работодателите по силата на Общия регламент относно защитата на данните. Освен това в него се изразяват повторно позицията и заключенията от Становище 8/2001 и Работен документ WP55, а именно че при обработването на личните данни на служителите:

- работодателите следва винаги да имат предвид основните принципи за защита на данните, независимо от използваната технология;
- съдържанието на електронните съобщения, изпратени от служебните помещения, е обхванато от същата защита на основните права като аналоговите съобщения;
- малко е вероятно съгласието да представлява валидно правно основание за обработването на данни на работното място, освен ако служителите могат да откажат, без това да доведе до неблагоприятни последици;
- понякога работодателят може да се позове на изпълнението на договор и на законни интереси, при условие че обработването е строго необходимо за законна цел и е в съответствие с принципите на пропорционалност и субсидиарност;
- служителите следва да получават ефективна информация относно наблюдението, което се извършва; както и
- всяко международно предаване на данни на служителите следва да се извършва само когато е гарантирано подходящо равнище на защита.

2. Въведение

Бързото възприемане на нови информационни технологии на работното място от гледна точка на инфраструктура, приложения и интелигентни устройства позволява

[1] РГ29, *Становище 08/2001 относно обработването на лични данни в контекста на трудово или служебно правоотношение*, WP48, 13 септември 2001 г., URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.

[2] РГ29, *Работен документ относно наблюдението на електронни съобщения на работното място*, WP55, 29 май 2002 г., URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf.

нови видове систематично обработване на данни на работното място, които потенциално могат да представляват намеса в личното пространство. Например:

- технологии, които позволяват обработването на данни на работното място, сега могат да се внедрят на много по-малка цена в сравнение с тази отпреди няколко години, докато капацитетът за обработване на лични данни чрез тези технологии се увеличи значително;
- новите форми на обработване, например свързаните с лични данни относно използването на онлайн услуги и/или с данни за местонахождение от интелигентно устройство, са много по-малко видими за служителите в сравнение с други по-традиционни видове, като например лесно забележимите камери на вътрешна система за видеонаблюдение. Това повдига въпроси за степента, в която служителите са запознати с тези технологии, тъй като е възможно работодателите да извършват това обработване незаконосъобразно, без да уведомяват предварително служителите; както и
- границите между личния и професионалния живот стават все по-неясни. Например, когато служителите работят дистанционно (например от дома си) или когато пътуват по служебни причини, може да се осъществява наблюдение на дейностите извън физическата работна среда и то потенциално може да включва наблюдение на лицето в личен контекст.

Поради това, макар че използването на такива технологии може да бъде от полза за откриването или предотвратяването на загуба на интелектуална и материална собственост на предприятието, за подобряване на производителността на служителите и за защита на личните данни, за които е отговорен администраторът, те също така пораждат значителни предизвикателства във връзка със защитата на данните и неприкосновеността на личния живот. В резултат на това е необходима нова оценка по отношение на баланса между законния интерес на работодателя да защити своя бизнес и разумните очаквания за неприкосновеността на личния живот от страна на субектите на данни: служителите.

Макар че настоящото становище ще бъде насочено най-вече към новите информационни технологии, като ще бъдат оценени девет различни сценария, в които те могат да се проявяват, в него също така ще се разгледат накратко по-традиционните методи за обработване на данни на работното място, когато в резултат на технологичните промени рисковете са засилени.

При използването на понятието „служител“ в настоящото становище РГ29 не възнамерява да ограничи обхвата на това понятие единствено до лица с трудов договор, признати като такива съгласно приложимото трудово право. През последните десетилетия по-често започнаха да се използват нови бизнес модели, при които възникват различни видове трудови правоотношения, и по-специално работа на свободна практика. Целта на настоящото становище е да се обхванат всички ситуации, в които са налице трудови правоотношения, независимо дали тези правоотношения се основават на трудов договор.

Важно е да се подчертае, че служителите рядко са в позиция да дават, отказват или оттеглят свободно своето съгласие с оглед на зависимостта, която възниква в резултат на отношенията работодател/служител. Освен в изключителни ситуации, работодателите трябва да се позовават на правно основание, различно от съгласие — като например необходимостта от обработване на данните в полза на техния законен

интерес. Наличието на законен интерес само по себе си обаче не е достатъчно, за да се получи преимущество пред правата и свободите на служителите.

Независимо от правното основание за такова обработване, преди да се пристъпи към него, е необходимо да се извърши проверка за пропорционалност, за да се прецени дали обработването е необходимо за постигане на законна цел, както и да се предприемат мерки, за да се гарантира, че нарушенията на правото на личен живот и тайната на съобщенията са сведени до минимум. Тази проверка може да представлява част от оценка на въздействието върху защитата на данните (ОВЗД).

3. Нормативна уредба

Макар че представеният по-долу анализ е извършен най-вече във връзка с настоящата нормативна уредба съгласно Директива 95/46/ЕО (Директивата за защита на личните данни или „ДЗЛД“)[3], в настоящото становище ще бъдат разгледани и задълженията съгласно Регламент 2016/679 (Общия регламент относно защитата на данните или „ОРЗД“)[4], който вече влезе в сила и ще започне да се прилага на 25 май 2018 г.

Що се отнася до предложението за регламент за неприкосновеността на личния живот и електронните съобщения[5], работната група призовава европейските законодатели да въведат специално изключение за вмешателство с устройства, които се предоставят на служителите[6]. Предложеният регламент не включва подходящо изключение от общата забрана за намеса и работодателите обикновено не могат да представят валидно съгласие за обработването на личните данни на своите служители.

3.1 Директива 95/46/ЕО — Директива за защита на личните данни (ДЗЛД)

В Становище 08/2001 РГ29 вече изтъкна, че работодателите би трябвало да вземат под внимание основните принципи на ДЗЛД във връзка със защитата на данните, когато обработват лични данни в контекста на трудово или служебно правоотношение. Развитието на нови технологии и нови методи за обработване в този контекст не са променили ситуацията — всъщност може да се заяви, че във връзка с това развитие стана *още по-важно* работодателите да правят това. В този контекст работодателите следва:

- да гарантират, че данните се обработват за конкретни и законни цели, които са пропорционални и необходими;

---

[3] Директива 95/46/ЕО от 24 октомври 1995 г. на Европейския парламент и на Съвета за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, *ОВ L 281, 23.11.1995 г., стр. 31—50*, URL: http://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex:31995L0046.

[4] 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 относно защитата на данните), *ОВ L 119, 4.5.2016 г., стр. 1—88*, URL: http://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016R0679.

[5] Предложение за регламент на Европейския парламент и на Съвета относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО, 2017/0003 (COD), URL: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[6] Вж. РГ29, *Становище 01/2017 относно предложението за регламент за неприкосновеността на личния живот и електронните съобщения*, WP247, 4 април 2017 г., стр. 29; URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

- да вземат предвид принципа за ограничаване в рамките на целта, като същевременно гарантират, че данните са подходящи, уместни и не са прекомерни за постигането на законната цел;
- да прилагат принципите на пропорционалност и субсидиарност независимо от приложимото правно основание;
- да осигурят в отношенията си със служителите прозрачност по отношение на използването и целите на технологиите за наблюдение;
- да създадат условия за упражняването на правата на субектите на данни, включително правото на достъп и по целесъобразност коригирането, изтриването или блокирането на лични данни;
- да поддържат данните точни и да не ги запазват за срок, по-дълъг отколкото е необходимо; както и
- да вземат всички необходими мерки за защита на данните от непозволен достъп и да гарантират, че персоналът е достатъчно добре запознат със задълженията за защита на данните.

Без да повтаря вече отправените съвети, РГ29 желае да подчертае три принципа, а именно: правно основание, прозрачност и автоматизирани решения.

3.1.1 *ПРАВНО ОСНОВАНИЕ (ЧЛЕН 7)*

Когато се обработват лични данни в контекста на трудово или служебно правоотношение, трябва да бъде изпълнен поне един от критериите, определени в член 7. Ако видът на обработваните лични данни включва специалните категории (описани в член 8), обработването е забранено, освен ако се прилага изключение[7,8]. Дори ако работодателят може да се позове на някое от тези изключения, продължава да се изисква правно основание по член 7, за да бъде обработването законосъобразно.

Накратко, поради тази причина работодателите трябва да отчетат следното:

- за по-голямата част от това обработване на данни на работното място **правното основание не може и не следва да бъде съгласието на служителите** (член 7, буква а) поради естеството на отношенията между работодател и служител;
- обработването може да бъде необходимо за **изпълнението на договор** (член 7, буква б) в случаите, когато работодателят трябва да обработва личните данни на служителя, за да изпълни тези задължения;
- доста често **може да се въвеждат правни задължения по силата на трудовото право** (член 7, буква в), **които налагат обработването на лични данни**; в тези случаи служителят трябва да получи ясна и пълна информация относно обработването (освен ако се прилага изключение);
- ако работодателят желае да се позове на **законен интерес** (член 7, буква е), целта на обработването трябва да бъде законна; избраният метод или конкретна

[7] Както се посочва в част 8 от Становище 08/2001; например в член 8, параграф 2, буква б) се предвижда изключение за целите на изпълнението на задълженията и специфичните права на администратора в областта на трудовото право, доколкото това е позволено от националното законодателство, което предвижда достатъчни гаранции за защита.

[8] Следва да се отбележи, че в някои държави са въведени специални мерки, които работодателите трябва да спазват с цел защита на личния живот на служителите. Португалия е една от държавите, в които съществуват такива специални мерки, а в някои други държави членки може да се прилагат сходни мерки. Поради това заключенията в раздел 5.6, както и примерите, представени в раздели 5.1 и 5.7.1 от настоящото становище, не са валидни за Португалия поради тези причини.

технология трябва да бъдат необходими, пропорционални и да се използват така, че да водят до възможно най-малка намеса, като същевременно трябва да позволяват на работодателя да демонстрира, че са **взети подходящи мерки**, за да се гарантира баланс с основните права и свободи на служителите[9];

- операциите по обработване също така трябва да отговарят на **изискванията за прозрачност** (членове 10 и 11) и служителите трябва да получат ясна и пълна информация относно обработването на техните лични данни[10], включително извършването на евентуално наблюдение; както и
- следва да се предприемат **подходящи технически и организационни мерки**, за да се гарантира надеждността на обработването (член 17).

По-долу са описани по-подробно най-релевантните критерии съгласно член 7.

- **Съгласие (член 7, буква а)**

В съответствие с ДЗЛД съгласието се определя като свободно изразено, конкретно и информирано указание за волята на съответното физическо лице, с което то дава израз на своето съгласие за обработка на личните данни, които се отнасят до него. За да бъде валидно съгласието, то трябва също така да може да бъде оттеглено.

В Становище 8/2001 РГ29 вече посочи, че когато работодателят трябва да обработва личните данни на своите служители, е подвеждащо да се тръгне от допускането, че обработването може да бъде легитимирано чрез съгласието на служителите. В случаите, когато работодателят заяви, че му е необходимо съгласие, и непредоставянето на съгласието е свързано с действителни или потенциални вреди за служителя (което е много вероятно в контекста на трудово или служебно правоотношение, особено когато става въпрос за проследяване от работодателя на поведението на служителя във времето), съгласието не е валидно, тъй като не е и не може да бъде свободно изразено. Следователно в повечето случаи, в които се обработват данни на служителите, правното основание за това обработване не може и не следва да бъде съгласието на служителите, поради което е необходимо друго правно основание.

Освен това дори в случаите, в които може да се твърди, че съгласието е валидно правно основание за такова обработване (т.е. ако може категорично да се заключи, че съгласието е свободно изразено), то трябва да представлява конкретно и информирано указание за волята на служителя. Настройките по подразбиране на устройства и/или инсталирането на софтуер, който улеснява обработването на лични данни в електронен вид, не могат да бъдат счетени за съгласие, дадено от служителите, тъй като съгласието изисква активно изразяване на волята. Липсата на действие (т.е. ако не се променят

[9] РГ29, *Становище 06/2014 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО*, WP217, прието на 9 април 2014 г., URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_bg.pdf.

[10] Съгласно член 11, параграф 2 от ДЗЛД администраторът е освободен от задължението за предоставяне на информация на субекта на данни в случаите, когато записът или събирането на данните е постановено изрично от закона.

настройките по подразбиране) като цяло не може да бъде счетена за конкретно съгласие за разрешаването на такова обработване[11].

- **Изпълнение на договор (член 7, буква б)**

Трудовите правоотношения често се основават на трудов договор между работодателя и служителя. Когато изпълнява задължения съгласно този договор, например заплащане на служителя, работодателят е длъжен да обработи някои лични данни.

- **Правни задължения (член 7, буква в)**

Доста често по силата на трудовото право се въвеждат правни задължения за работодателя, които налагат обработването на лични данни (например за целите на изчисляването на данъка или за административни дейности във връзка със заплатите). Очевидно в тези случаи въпросното законодателство представлява правното основание за обработването на данните.

- **Законен интерес (член 7, буква е)**

Ако работодателят желае да се позове на правното основание, посочено в член 7, буква е) от ДЗЛД, целта на обработването трябва да бъде законна и избраният метод или конкретната технология, чрез които ще се извършва обработването, трябва да бъдат необходими за законния интерес на работодателя. Освен това обработването трябва да бъде пропорционално на потребностите на предприятията, т.е. на целта, за която се извършва. Обработването на данни на работното място следва да се извършва с възможно най-малка намеса и да бъде насочено към конкретната област на риск. Освен това при позоваване на член 7, буква е) се запазва правото на служителя на възражение срещу обработването въз основа на неопровержими законови основания съгласно член 14.

За да се използва член 7, буква е) като правно основание за обработването, е изключително важно да бъдат въведени конкретни смекчаващи мерки, така че да се гарантира подходящ баланс между законния интерес на работодателя и основните права и свободи на служителите[12]. В зависимост от формата на наблюдение тези мерки следва да включват ограничения по отношение на наблюдението, така че да се гарантира, че не се нарушава неприкосновеността на личния живот на служителя. Такива ограничения биха могли да бъдат:

- географски (например наблюдение само на определени места; следва да бъде забранено наблюдението на чувствителни зони, като например религиозни обекти, санитарни помещения и стаи за отдих),

[11] Вж. също така РГ29, *Становище 15/2011 относно понятието „съгласие“*, WP187, 13 юли 2011 г., URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_bg.pdf, стр. 24.

[12] За пример относно баланса, който трябва да бъде постигнат, вж. решение на ЕСПЧ от 5 октомври 2010 г., *Köpke/Германия*, 1725 (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), в случая по което служител е бил уволнен в резултат на операция по видеонаблюдение под прикритие, предприета от работодателя и частна детективска агенция. Макар че в този случай Съдът заключи, че националните органи са постигнали подходящ баланс между законния интерес на работодателя (в защита на неговите права на собственост), правото на зачитане на личния живот на служителя и обществения интерес за правораздаване, той също така отбеляза, че тежестта на тези различни интереси може да се промени в бъдеще в резултат на развитието на технологиите.

- по отношение на данните (например не следва да подлежат на наблюдение лични електронни файлове и съобщения), и
- свързани с времето (например извадки вместо непрекъснато наблюдение).

3.1.2 *Прозрачност (членове 10 и 11)*

Изискванията за прозрачност, посочени в членове 10 и 11, се прилагат към обработването на данни на работното място; служителите трябва да получат информация относно извършването на евентуално наблюдение, относно целите, за които ще се обработват личните данни, както и всякаква друга информация, която е необходима, за да се гарантира добросъвестно обработване.

Необходимостта от прозрачност става по-очевидна с навлизането на нови технологии, тъй като те позволяват събирането и по-нататъшното обработване на евентуално огромни количества лични данни по прикрит начин.

3.1.3 *Автоматизирани решения (член 15)*

Член 15 от ДЗЛД също така осигурява на субектите на данни правото да не бъдат обект на решение, което се основава единствено на автоматизирана обработка, когато това решение има правни последици за тях или ги засяга съществено, и което се основава единствено на автоматизираната обработка на данни, имаща за цел да се оценяват някои лични аспекти като резултатите от работата, освен ако решението е необходимо за сключване или изпълнение на договор, разрешено е съгласно правото на Съюза или на държавата членка или се основава на изричното съгласие на субекта на данни.

3.2 Регламент 2016/679/ — Общ регламент относно защитата на данните („ОРЗД“)

ОРЗД включва и разширява изискванията, посочени в ДЗЛД. Освен това той въвежда нови задължения за всички администратори на данни, включително работодателите.

3.2.1 *Защита на данните на етапа на проектирането*

Съгласно член 25 от ОРЗД от администраторите се изисква да въвеждат мерки за защита на данните на етапа на проектирането и по подразбиране. Ето един пример: когато работодателят предоставя устройства на служителите, следва да бъдат избрани решенията, които благоприятстват в най-висока степен защитата на неприкосновеността на личния живот, ако в съответните случаи се използват технологии за проследяване. Свеждането на данните до минимум също трябва да се вземе предвид.

3.2.2 *Оценки на въздействието върху защитата на данните*

В член 35 от ОРЗД се посочват изискванията по отношение на администратора във връзка с извършването на оценка на въздействието върху защитата на данните (ОВЗД), когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица. Пример за това е систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично обработване, включително

профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице.

Когато ОВЗД показва, че идентифицираните рискове не могат да се ограничат в достатъчна степен от администратора — т.е. остатъчните рискове остават високи — администраторът трябва да се консултира с надзорния орган, преди да започне обработването (член 36, параграф 1), както се пояснява в насоките на РГ29 относно ОВЗД[13].

3.2.2 „*ОБРАБОТВАНЕ В КОНТЕКСТА НА ТРУДОВО ИЛИ СЛУЖЕБНО ПРАВООТНОШЕНИЕ*“

Член 88 от ОРЗД гласи, че държавите членки могат със закон или с колективни споразумения да предвидят по-конкретни правила, за да гарантират защитата на правата и свободите по отношение на обработването на личните данни на наетите лица по трудово или служебно правоотношение. По-специално такива правила могат да бъдат предвидени за целите на:

- набирането на персонал;
- изпълнението на трудовия договор (включително изпълнението на задълженията, установени със закон или с колективни споразумения);
- управлението, планирането и организацията на работата;
- равенството и многообразието на работното място;
- здравословните и безопасни условия на труд;
- защитата на имуществото на работодателя или на клиента;
- упражняване и ползване (на индивидуална основа) на правата и облагите, свързани със заетостта; както и
- прекратяване на трудовото или служебното правоотношение.

В съответствие с член 88, параграф 2 тези правила следва да включват подходящи и конкретни мерки за защита на човешкото достойнство, законните интереси и основните права на субекта на данните, по-специално по отношение на:

- прозрачността на обработването;
- предаването на лични данни в рамките на група предприятия или група дружества, участващи в съвместна стопанска дейност; и
- системите за наблюдение на работното място.

В настоящото становище работната група предоставя насоки за законосъобразното използване на нови технологии в редица конкретни ситуации, като се описват подробно подходящи и конкретни мерки за защита на човешкото достойнство, законните интереси и основните права на служителите.

4. Рискове

Съвременните технологии дават възможност за проследяване на служителите във времето на работното им място и в домовете им посредством множество различни

[13] РГ29, *Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679*, WP248, 4 април 2017 г., URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, стр. 18.

устройства като смартфони, настолни или таблетни компютри, превозни средства и носими устройства. Ако не съществуват ограничения за обработването и ако то не е прозрачно, съществува висок риск законният интерес на работодателите за подобряване на ефикасността и защитата на активите на дружеството да се превърне в неоправдано наблюдение, което представлява намеса в личното пространство.

Технологиите за наблюдение на съобщенията също могат да окажат възпиращо въздействие върху упражняването от служителите на техните основни права да се организират, да провеждат срещи на работниците и да общуват в условията на поверителност (включително върху упражняването на правото на търсене на информация). Наблюдението на съобщенията и на поведението би оказало натиск върху служителите да спазват правилата, за да избегнат разкриването на действия, които могат да се възприемат като нередни, подобно на начина, по който засиленото използване на вътрешна система за видеонаблюдение повлия върху поведението на гражданите на обществени места. Освен това поради възможностите на тези технологии би могло служителите да не са наясно какви лични данни се обработват и за какви цели, а същевременно е възможно дори да не знаят за съществуването на самата технология за наблюдение.

Използването на информационни технологии за наблюдение също така се различава от други, по-лесно забележими инструменти за наблюдение и мониторинг, като например вътрешна система за видеонаблюдение, тъй като може да се извършва прикрито. При отсъствието на лесно разбираема и достъпна политика за наблюдение на работното място служителите може да не знаят за съществуването и последиците от извършваното наблюдение и поради това да не са в състояние да упражнят своите права. Допълнителен риск се поражда от прекомерното събиране на данни в такива системи, например тези, с които се събират данни за местонахождението на устройства с WiFi.

Нарастването на обема на данните, генерирани на работното място, в съчетание с новите техники за анализ и установяване на съвпадения на данни също така могат да породят рискове от несъвместимо по-нататъшно обработване. Примерите за незаконосъобразно по-нататъшно обработване включват използването на системи, които са законно инсталирани с цел защита на имуществото, за наблюдение кога служителите са на място, как работят и доколко са вежливи с клиентите. Други примери включват използването на данни, събрани чрез вътрешна система за видеонаблюдение, за периодично наблюдение на поведението и работата на служителите, или използването на данни от система за определяне на географското местоположение (например чрез проследяване чрез WiFi или Bluetooth) за непрекъснати проверки на движението и поведението на служителите.

Такова проследяване може като резултат да наруши правата за неприкосновеност на личния живот на служителите, независимо дали се извършва систематично или само понякога. Рискът не е ограничен до анализа на съдържанието на съобщенията. По този начин анализът на метаданните относно дадено лице може да позволи подробно наблюдение със също толкова сериозна намеса в личното пространство по отношение на живота и поведенческите модели на дадено лице.

Широкообхватното използване на технологии за наблюдение също така може да ограничи готовността на служителите (и възможните канали) да информират работодателите относно нередности или незаконни действия на своите ръководители

и/или други служители, които пораждат риск от причиняване на вреди на предприятието (особено данни за клиенти) или на работното място. Често е необходима анонимност, така че съответният служител да предприеме действия и да съобщи за такива ситуации. Наблюдение, което нарушава правата на неприкосновеност на личния живот на служителите, може да възпрепятства подаването на сигнали към съответните длъжностни лица. В такъв случай установената система за сигнализиране на нередности от вътрешни лица може да изгуби своята ефективност[14].

5. Сценарии

В настоящия раздел се разглеждат редица сценарии с обработване на данни на работното място, в които новите технологии и/или усъвършенстването на съществуващите технологии разполагат или може да разполагат с потенциал да породят високи рискове за неприкосновеността на личния живот на служителите. Във всеки от тези случаи работодателите следва да обмислят дали:

- дейността по обработване е необходима и ако това е така, какви правни основания се прилагат;
- предложеното обработване на лични данни е справедливо за служителите;
- дейността по обработване е пропорционална на породилите се опасения; и
- дейността по обработване е прозрачна.

5.1 Операции по обработване по време на процедурата по набиране на персонал

Широкоразпространено е използването на социални медии от физическите лица, като относително често профилите на потребителите са публично достъпни в зависимост от настройките, избрани от титуляря на акаунта. В резултат на това работодателите може да бъдат на мнение, че проучването на социалните профили на потенциалните кандидати може да бъде обосновано по време на процедурата по набиране на персонал. Такъв може да бъде случаят и по отношение на друга публично достъпна информация относно потенциалния служител.

При все това работодателите не следва да приемат, че имат право да обработват тези данни за свои собствени цели само защото профилът на дадено лице в социална медия е публично достъпен. За това обработване се изисква правно основание, като например законен интерес. В този контекст работодателят следва — преди проверката на профил в социална медия — да вземе предвид дали профилът на кандидата в социалната медия е свързан със служебни или лични цели, тъй като това може да бъде важен показател за правната допустимост на проверката на данните. Освен това работодателите имат право да събират и обработват лични данни във връзка с кандидати за работа само до степента, в която събирането на тези данни е необходимо и уместно за изпълнението на работата, за която кандидатства лицето.

[14] Вж. например РГ29, *Становище 1/2006 относно прилагането на правилата на ЕС за защита на данните по отношение на вътрешните схеми за подаване на сигнали за нарушения в областта на счетоводството, вътрешния счетоводен контрол, одитите, борбата срещу корупцията, банковите и финансовите престъпления*, WP117, 1 февруари 2006 г., URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.

Данните, събрани по време на процедурата по набиране на персонал, като цяло следва да се заличат веднага след като стане ясно, че няма да бъде отправено предложение за работа или че то не е прието от съответното лице[15]. Освен това лицето трябва да бъде правилно информирано относно това обработване, преди да се пристъпи към процедурата по набиране на персонал.

Не съществува правно основание, съгласно което работодателят може да изисква потенциалните служители да приемат покана за приятелство от потенциалния работодател в социалните медии, нито по друг начин да предоставят достъп до съдържанието на своите профили.

Пример

По време на набирането на нов персонал даден работодател проверява профилите на кандидатите в различни социални медии и включва информация от тези медии (и всякаква друга информация, достъпна в интернет) в процеса на проучване.

Работодателят може да разполага с правно основание съгласно член 7, буква е) да преглежда публично достъпна информация относно кандидатите само ако прегледът на информация относно даден кандидат в социалните медии е необходим за самата работа, например, за да може да се оценят конкретни рискове във връзка с кандидатите за специфична задача, и само ако кандидатите са правилно информирани (например в текста на обявлението за работа).

[15] Вж. също така Съвет на Европа, *Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment* (Препоръка CM/Rec(2015)5 на Комитета на министрите към държавите членки относно обработването на лични данни в контекста на трудово или служебно правоотношение), точка 13.2 (1 април 2015 г., URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). Когато работодателят желае да запази данните с цел последваща възможност за работа, субектът на данни следва да бъде информиран по съответния начин и да му бъде дадена възможност да възрази срещу такова по-нататъшно обработване, като в случай на възражение данните следва да бъдат заличени (пак там).

5.2 Операции по обработване в резултат на проверка в контекста на трудово или служебно правоотношение

В резултат на съществуването на профили в социалните медии и развитието на нови аналитични технологии работодателите разполагат (или могат да се сдобият със) техническата възможност, постоянно да проверяват служителите, като събират информация във връзка с техните приятели, мнения, убеждения, интереси, навици, местонахождение, отношения и поведение, като по този начин събират данни, включително чувствителни данни, свързани с личния и семейния живот на служителя.

Проверките в контекста на трудово или служебно правоотношение на профилите на служителите в социалните медии не следва да се извършват на обща основа.

Освен това работодателите следва да се въздържат да изискват служителят или кандидатът за работа да им предостави достъп до информация, която споделя с други лица чрез социалните медии.

Пример
Работодател наблюдава профилите в LinkedIn на бивши служители, които са подписали клаузи за въздържане от конкуренция за определен период. Целта на това наблюдение е да се проследява спазването на тези клаузи. Наблюдението е ограничено до тези бивши служители.

При условие че работодателят може да докаже, че това наблюдение е необходимо за защита на неговите законни интереси и че не съществуват други начини с по-малка намеса, както и че бившите служители са били информирани по подходящ начин относно степента на редовното наблюдение на техните публични съобщения, работодателят може да се позове на правното основание на член 7, буква е) от ДЗЛД.

Освен това от служителите не следва да се изисква да използват осигурени от техния работодател профили в социалните медии. Дори когато това специално се предвижда в контекста на техните задачи (например говорител на организация), те трябва да имат възможност за профил, който не е „служебен“ и публичен, и който могат да използват вместо „официалния“ профил, свързан с работодателя, като това следва да бъде посочено в условията на трудовия договор.

5.3 Операции по обработване в резултат на използването на ИКТ за наблюдение на работното място

Традиционно наблюдението на електронните съобщения на работното място (например телефон, използване на интернет, електронна поща, съобщения в реално време, интернет телефония и др.) се считаше за основната заплаха за неприкосновеността на личния живот на служителите. В приетия през от 2001 г. *Работен документ относно наблюдението на електронни съобщения на работното място* РГ29 достигна до редица заключения във връзка с наблюдението на електронни пощи и използването на интернет. Макар че тези заключения продължават да бъдат валидни, трябва да се отчетат и технологичните развития, които създадоха условия за по-нови начини за наблюдение с потенциално по-голяма намеса и по-всестранно. Тези развития включват наред с другото:

- инструменти за предотвратяване на загуба на данни (DLP), с които се следят изходящи съобщения с цел откриване на потенциални нарушения на сигурността на данните;
- защитни стени от следващо поколение (NGFW) и системи за унифицирано управление на заплахите (UTM), които могат да осигурят разнообразие от технологии за наблюдение, включително задълбочена проверка на пакети, прихващане на TLS трафик, филтриране на уебсайтове, филтриране на съдържание, доклади за употребата в самото устройство, информация за самоличността на потребителя и (както е описано по-горе) предотвратяване на загуба на данни. Такива технологии могат да бъдат въведени и поотделно в зависимост от работодателя;
- приложения и мерки за сигурност, които включват записване на достъпа на служителите до системите на работодателя;
- технологии за електронно разследване, което се отнася до всеки процес, при който се претърсват електронни данни с цел използването им като доказателство;
- проследяване на използването на приложения и устройства чрез невидим софтуер, инсталиран на настолния компютър или в облака;
- използване на предвидени за използване в офиса приложения на работното място, предоставяни като услуги за изчисления в облака, което на теория позволява изключително подробно записване на дейностите на служителите;
- наблюдение на лични устройства (например персонални компютри, мобилни телефони, таблети), с които служителите се снабдяват за своята работа в съответствие с конкретна политика за ползване, като например принципа „Донеси своето собствено устройство“ (BYOD), както и технологии за управление на мобилни устройства (MDM), които позволяват разпространение на приложения, данни и настройки за конфигурация, както и актуализации за мобилни устройства; и
- използване на носими устройства (например устройства, свързани със здраве и фитнес).

Възможно е работодателите да прилагат „пакетно“ решение за наблюдение, като например набор от пакети с мерки за сигурност, които им позволяват да наблюдават цялостното използване на ИКТ на работното място, а не само наблюдение на електронна поща и/или уебсайтове, какъвто бе случаят преди. Заключенията, приети в документ WP55, са приложими за всяка система, която позволява извършването на такова наблюдение[16].

Пример

Работодател възнамерява да въведе устройство за проверка на TLS трафик за декодиране и проверка на защитен трафик с цел откриване на евентуални злонамерени действия. Устройството също така е в състояние да записва и анализира цялата онлайн дейност на служителя в мрежата на организацията.

[16] Вж. също така решение на ЕСПЧ от 3 април 2007 г., *Copland/Обединено кралство,* (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, 253 (URL: http://www.bailii.org/eu/cases/ECHR/2007/253.html), в което Съдът постанови, че електронните писма, които се изпращат от служебните помещения, и информацията, получена от наблюдение на използването на интернет, биха могли да представляват част от личния живот и кореспонденцията на служителя, и че събирането и съхранението на тази информация без знанието на служителя би представлявало вмешателство в правата на служителя, макар че Съдът не постанови, че такова наблюдение никога няма да бъде необходимо в едно демократично общество.

Все по-често се прибягва до използването на протоколи за криптирана комуникация с цел защита срещу прихващане на потоци от онлайн данни, които включват лични данни. Това обаче също може да породи проблеми, тъй като криптирането прави невъзможно наблюдението на входящите и изходящите данни. Оборудването за проверка на TLS декодира потока от данни, анализира съдържанието за целите на сигурността и след това повторно криптира потока.

В този пример работодателят се позовава на законни интереси — необходимостта да защити мрежата и личните данни на служителите и клиентите, които са в рамките на тази мрежа, от непозволен достъп или изтичане на данни. При все това наблюдението на всички онлайн дейности на служителите е непропорционално решение и представлява вмешателство в правото на тайна на съобщенията. Работодателят следва първо да проучи други средства с по-малка намеса, с които да защити поверителността на данните на клиентите и сигурността на мрежата.

До степента, в която известно прихващане на TLS трафик може да бъде окачествено като строго необходимо, устройството следва да бъде настроено по такъв начин, че да се избегне постоянното записване на дейността на служителите, например чрез блокиране на съмнителен входящ или изходящ трафик и пренасочване на потребителя към информационен портал, където той може да поиска преразглеждане на това автоматизирано решение. Ако независимо от това бъде счетено, че е строго необходимо да се извършва общо записване в някаква степен, устройството също така може да бъде настроено да не съхранява записаните данни, освен ако сигнализира за инцидент, като събраната информация се свежда до минимум.

Като добра практика работодателят би могъл да предложи за служителите алтернативен достъп без наблюдение. Това би могло да се извърши чрез осигуряване на безплатни, самостоятелни устройства или терминали, или такива с WiFi (с подходящи предпазни мерки, за да се гарантира поверителността на съобщенията), като по този начин служителите могат да упражняват законното си право да използват съоръжения в работата за някои лични нужди[17]. Освен това работодателите следва да проучат някои видове трафик, чието прихващане застрашава правилния баланс между техните законни интереси и неприкосновеността на личния живот на служителите — например използването на частни уеб-базирани пощи, посещения на здравни уебсайтове и уебсайтове за онлайн банкиране — с цел да настроят устройството по подходящ начин, така че да не се прихващат съобщения при обстоятелства, които не отговарят на принципа на пропорционалност. На служителите следва да бъде предоставена информация относно вида съобщения, които се следят от устройството.

Следва да бъде разработена политика за целите, за които може да се осъществява достъп до записи на съмнителни данни, и за лицата, които могат да осъществяват достъп до тях, като тази политика следва да бъде лесно и постоянно достъпна за всички служители, за да може да ги насочва относно приемливото и неприемливото

[17] Вж. решение на ЕСПЧ от 25 юни 1997 г., *Halford/Обединено кралство*, 32 (URL: http://www.bailii.org/eu/cases/ECHR/1997/32.html), в което Съдът постанови, че „телефонни разговори, осъществени от служебни помещения, както и от дома, могат да бъдат обхванати от понятията „личен живот“ и „кореспонденция“ по смисъла на член 8, параграф 1 [от Конвенцията]“; и решение на ЕСПЧ от 12 януари 2016 г., *Barbulescu/Румъния*, 61 (URL: http://www.bailii.org/eu/cases/ECHR/2016/61.html), свързано с използването на служебен акаунт в приложение за съобщения в реално време за лична кореспонденция, в което Съдът заяви, че наблюдението на акаунта от работодателя е ограничено и пропорционално; особеното мнение на съдия Pinto de Alberquerque, в което се призовава за постигане на точен баланс.

използване на мрежата и съоръженията. Това позволява на служителите да пригодят своето поведение, така че да се избегне наблюдението им, когато законно използват ИТ съоръженията в работата за лични нужди. Като добра практика такава политика следва да се оценява поне веднъж годишно, за да се прецени дали избраното решение за наблюдение води до очакваните резултати, и дали са достъпни други средства или начини с по-малка намеса, с които могат да се постигнат същите цели.

Независимо от съответната технология и възможностите, с които тя разполага, правното основание в член 7, буква е) може да се използва само ако обработването отговаря на определени условия. Първо, работодателите, които използват тези продукти и приложения, трябва да проучат пропорционалността на прилаганите от тях мерки и дали могат да бъдат предприети допълнителни действия за смекчаване или ограничаване на мащаба и въздействието от обработването на данни. Като пример за добра практика това проучване би могло да се извърши посредством ОВЗД, преди да бъде въведена технология за наблюдение. Второ, работодателите трябва да въведат и съобщят политики за приемливо използване успоредно с политики за неприкосновеност на личния живот, в които се посочва допустимото използване на мрежата и оборудването на организацията и подробно се описва обработването, което се извършва.

В някои държави за създаването на такава политика законово се изисква одобрението на работнически съвет или подобно представителство на служителите. На практика такива политики често се изготвят от персонала за ИТ поддръжка. Тъй като те са насочени най-вече към аспектите на сигурността, а не към законните очаквания на служителите за неприкосновеност на личния им живот, РГ29 препоръчва във всички случаи при оценяването на необходимостта от наблюдение, както и на логиката и достъпността на политиката да бъде включена представителна извадка от служителите.

Пример

Работодател въвежда инструмент за предотвратяване на загуба на данни, за да наблюдава автоматично изходящите електронни писма с цел предотвратяване на непозволено предаване на данни, които са обект на права на собственост (например лични данни на клиентите), независимо дали тези действия са умишлени или не. Ако дадено електронно писмо бъде счетено за потенциален източник на нарушение на сигурността на данните, се извършва последващо разследване.

И в този случай работодателят се позовава на необходимостта от своя законен интерес да защити личните данни на клиентите, както и своите активи от непозволен достъп или изтичане на данни. Такъв инструмент за DLP обаче може да включва ненужно обработване на лични данни — например лъжлив положителен сигнал може да доведе до осъществяване на непозволен достъп до законни електронни писма, изпратени от служителите (които например могат да бъдат лични електронни писма).

Поради това необходимостта от инструмент за DLP и неговото въвеждане следва да бъде напълно обоснована, така че да се постигне подходящ баланс между законните интереси на работодателя и основното право за защита на личните данни на служителите. За да може работодателят да се позове на законни интереси, следва да се предприемат определени мерки за ограничаване на рисковете. Например правилата, които следва системата, когато обозначава електронно писмо като потенциално нарушение на сигурността на данните, следва да бъдат напълно прозрачни за потребителите, а в случай че инструментът установи, че с дадено електронно писмо, което предстои да бъде изпратено, евентуално се нарушава сигурността на данните, изпращачът на електронното писмо следва да получи предупредително съобщение преди изпращането на електронното писмо, за да му се даде възможност да отмени изпращането.

В някои случаи наблюдението на служители е възможно не толкова заради въвеждането на специфични технологии, а просто защото от служителите се очаква да използват предоставени от работодателя онлайн приложения, които обработват лични данни. Пример за това е използването на офис приложения в облака (например текстообработващи програми, календари, социални медии). Следва да се гарантира, че служителите могат да посочват определени лични пространства, до които работодателят не може да получи достъп, освен при извънредни обстоятелства. Това например е уместно за календарите, които често се използват и за лични ангажименти. Ако служителят обозначи даден ангажимент като „личен“ или отбележи това в самия ангажимент, на работодателите (и на останалите служители) не следва да се позволява да разглеждат съдържанието на ангажимента.

Изискването за субсидиарност в този контекст понякога означава, че изобщо не може да се извършва наблюдение. Например такъв е случаят, когато забраненото използване на съобщителни услуги може да бъде предотвратено чрез блокиране на определени уебсайтове. Ако е възможно да се блокират уебсайтове, вместо да се извършва непрекъснато наблюдение на всички съобщения, следва да бъде предпочетено блокирането, за да се спази това изискване за субсидиарност.

В по-общ план следва да бъде отдадено много по-голямо значение на предотвратяването, отколкото на разкриването — интересите на работодателя се обслужват по-добре чрез предотвратяване на злоупотребата с интернет с помощта на технически средства, отколкото чрез изразходване на ресурси за откриване на злоупотреби.

5.4 Операции по обработване в резултат на използването на ИКТ за наблюдение извън работното място

Използването на ИКТ извън работното място започна да се среща по-често с нарастването на работата от дома, дистанционната работа и политиките „Донеси своето собствено устройство“. Възможностите на тези технологии могат да породят риск за личния живот на служителите, тъй като в много случаи системите за наблюдение, въведени на работното място, на практика обхващат и личната сфера на служителите, когато използват такова оборудване. .

5.4.1 *НАБЛЮДЕНИЕ ПРИ РАБОТА ОТ ДОМА И ДИСТАНЦИОННА РАБОТА*

За работодателите стана обичайна практика да предлагат на служителите възможността да работят дистанционно, т.е. от дома и/или докато пътуват. В действителност това е основен фактор за намаляване на разграничението между работното място и дома. Като цяло в тази връзка работодателят предоставя ИКТ оборудване или софтуер на служителите и след като бъдат поставени в дома на служителя или на неговите устройства, в зависимост от използвания метод те му осигуряват същото ниво на достъп до мрежата, системите и ресурсите на работодателя, с каквото би разполагал на работното място.

Макар че дистанционната работа може да представлява положително развитие, тя представлява и област на допълнителен риск за работодателя. Например служители, които разполагат с дистанционен достъп до инфраструктурата на работодателя, не са ограничени от физическите мерки за сигурност, които могат да се прилагат в помещенията на работодателя. С други думи: без въвеждането на подходящи технически мерки рискът от непозволен достъп се повишава, като може да доведе до загубата или унищожаването на информация, включително лични данни на служители или клиенти, с които работодателят може да разполага.

За да ограничат тази област на риск, работодателите може да решат, че е оправдано да използват софтуерни пакети (било то в помещенията, или в облака), които разполагат например с възможност да записват натисканията на клавишите и движението на мишката, да правят моментни снимки на екрана (на случаен принцип или на определени интервали), да записват използваните приложения (и времето, за което са използвани), а в случай на съвместими устройства да включват уебкамери и да събират записите от тях. Такива технологии са достъпни от много места, включително от трети страни, като например доставчици на услуги за изчисления в облака.

При все това обработването, свързано с тези технологии, е непропорционално и е много малко вероятно законният интерес на работодателя да представлява валидно правно основание, например за записване на натисканията на клавишите и движението на мишката.

Ключът е да се отстрани породеният от работата от дома и дистанционната работа риск по пропорционален и непрекомерен начин независимо от предложения вариант и технология, особено ако границите между служебното и личното ползване не са строго определени.

5.4.2 *„ДОНЕСИ СВОЕТО СОБСТВЕНО УСТРОЙСТВО“ (BYOD)*

Поради това, че се увеличават популярността, функциите и възможностите на електронните устройства за потребители, служителите могат да поискат от

работодателите да използват свои собствени устройства на работното място, за да изпълняват своята работа. Този принцип е известен като „Донеси своето собствено устройство“ или BYOD.

Въвеждането на BYOD на практика може да доведе до редица ползи за служителите, включително повишена удовлетвореност от работата, цялостно повдигане на духа, подобрена ефикасност на работата и повишена гъвкавост. При все това по подразбиране устройството на служителя в известна степен ще се ползва и за лични цели, какъвто е по-вероятно да бъде случаят в определени периоди от денонощието (например вечер или през почивните дни). Поради това съществува реална възможност, в резултат на използването от служителите на техни собствени устройства работодателите да обработват неслужебна информация относно тези служители и евентуално членове на семейството, които също използват въпросните устройства.

В контекста на трудово или служебно правоотношение произтичащите от BYOD рискове за неприкосновеността на личния живот са свързани най-вече с технологии за наблюдение, които събират идентификатори, като например MAC адреси, или в случаите, когато работодателят осъществява достъп до устройството на служителя на основание, че извършва сканиране за целите на сигурността, т.е. за зловреден софтуер. По отношение на последното съществуват редица търговски решения, които позволяват сканиране на лични устройства, но с тяхното използване потенциално би могъл да се осъществи достъп до всички данни на устройството и поради това те трябва да се управляват внимателно. Например, по принцип не може да се осъществява достъп до определено пространство на дадено устройство, което предполагаемо се използва само за лични цели (например папката, в която се съхраняват снимки, направени с устройството).

Може да бъде счетено, че наблюдението на местонахождението на такива устройства и на техния трафик обслужва законен интерес за защита на личните данни, за които работодателят носи отговорност като администратор на данни; това обаче може да бъде незаконосъобразно, когато става въпрос за личното устройство на служителя, ако при такова наблюдение се събират и данни, свързани с личния и семейния живот на служителя. За да се предотврати наблюдението на лична информация, трябва да се въведат подходящи мерки, с които да се разграничава личното и служебното използване на устройството.

Работодателите също така следва да използват методи, чрез които техните собствени данни на устройството се предават по сигурен начин между устройството и тяхната мрежа. Поради това е възможно устройството да бъде настроено по такъв начин, че целият трафик да минава през VPN обратно към корпоративната мрежа, с цел да се осигури определено равнище на сигурност; ако се използва такава мярка обаче, работодателят следва също така да обърне внимание на факта, че инсталираният софтуер за наблюдение поражда риск за неприкосновеността на личния живот в периодите, когато служителят използва устройството за лични цели. Биха могли да се използват устройства, които предлагат допълнителна защита, като например поставяне на данните в т. нар. „sandbox“ режим (ограничаване на данните в рамките на конкретно приложение).

От друга страна, работодателят също така трябва да обмисли дали да забрани използването на конкретни служебни устройства за частни цели, ако няма как да предотврати наблюдението на личното използване — например, ако устройството

предлага дистанционен достъп до лични данни, по отношение на които работодателят е администратор на данни.

5.4.3 *Управление на мобилни устройства (MDM)*

Управлението на мобилни устройства позволява на работодателите да установяват дистанционно местонахождението на устройствата, да въвеждат специфични конфигурации и/или да инсталират специфични приложения, както и да заличават данни при поискване. Работодателят може да управлява тази функция самостоятелно или да използва услугите на трета страна за тази цел. Услугите за MDM също така позволяват на работодателите да записват или проследяват устройството в реално време дори ако не е обявено за откраднато.

Преди разгръщането на такава технология, когато тя е нова или е нова за администратора, следва да се извърши ОВЗД. Ако резултатът от ОВЗД покаже, че технологията за MDM е необходима в определени обстоятелства, все пак следва да се извърши оценка дали произтичащото обработване на данни отговаря на принципите на пропорционалност и субсидиарност. Работодателите трябва да гарантират, че данните, които се събират като част от тази възможност за дистанционно определяне на местонахождението, се обработват за конкретна цел, като не представляват, нито биха могли да представляват, част от по-широкообхватна програма, позволяваща постоянно наблюдение на служителите. Функциите за проследяване следва да бъдат ограничени дори за конкретни цели. Системите за проследяване могат да бъдат проектирани да регистрират данни за местонахождението, без да ги представят на работодателя — при тези обстоятелства данните за местонахождението следва да станат достъпни само ако бъде подаден сигнал за нарушение или ако устройството бъде изгубено.

Служителите, чиито устройства са обхванати от услуги за MDM, също така трябва да бъдат напълно информирани какво проследяване се извършва и какви последици произтичат от него за тях.

5.4.4 *Носими устройства*

Работодателите все по-често се изкушават да предоставят носими устройства на своите служители, за да следят и наблюдават тяхното здравословно състояние и дейност в рамките на работното място, а понякога дори и извън него. Това обработване на данни обаче включва обработване на данни, свързани със здравословното състояние, и по тази причина е забранено въз основа на член 8 от ДЗЛД.

С оглед на неравнопоставените отношения между работодателите и служителите — т.е. служителят зависи от работодателя за своята заплата — и чувствителното естество на данните, свързани със здравословното състояние, изключително малко вероятно е да може да се даде валидно от законова точка и изрично съгласие за проследяването или наблюдението на такива данни, тъй като служителите по същество изобщо не са „свободни“ да изразят такова съгласие. Обработването ще бъде незаконосъобразно дори ако за събирането на данните, свързани със здравословното състояние, работодателят използва трета страна, която предоставя на работодателя единствено информация в обобщен вид относно промените в общото здравословно състояние.

Освен това, както е описано в *Становище 05/2014 относно техническите способи за анонимизиране*[18], от техническа гледна точка е изключително трудно да се гарантира пълно анонимизиране на данните. Дори в условията на среда с над хиляда служители, предвид наличието на други данни относно служителите, работодателят пак ще бъде в състояние да разграничи отделни служители с конкретни здравословни показатели, като например високо кръвно налягане или затлъстяване.

Пример:

Организация предлага като общ подарък на своите служители устройства за наблюдение, свързани с фитнес практики. Устройствата отчитат броя стъпки на служителите и постоянно регистрират сърдечния ритъм и качеството на съня.

Събраните данни, свързани със здравословното състояние, следва да бъдат достъпни само за служителя, но не и за работодателя. Въпросът за предаването на данни между служителя (като субект на данни) и доставчика на устройството/услугата (като администратор), се урежда между тези страни.

Тъй като данните, свързани със здравословното състояние, биха могли да се обработват от търговското предприятие, което е произвело устройствата или предлага услугата на работодателите, при избора на устройството или услугата работодателят следва да оцени политиката на производителя и/или доставчика на услуги по отношение на неприкосновеността на личния живот, за да гарантира, че тя няма да доведе до незаконосъобразно обработване на данни, свързани със здравословното състояние на служителите.

5.5 Операции по обработване, свързани с време и присъствие

Системите, които позволяват на работодателите да контролират кой може да влиза в техните помещения и/или в определени зони от техните помещения, също могат да позволят проследяване на дейностите на служителите. Въпреки че такива системи съществуват от много години, все по-често започват да се въвеждат нови технологии, насочени към проследяване на времето и присъствието, включително такива, които обработват биометрични данни, както и такива за проследяване на мобилни устройства.

Макар че такива системи могат да представляват важен елемент от одитната следа на работодателя, те също така пораждат риск от осигуряване на информираност и контрол на равнище, което предполага сериозна намеса, по отношение на дейностите на служителя, докато се намира на работното място.

Пример:

Работодател поддържа помещение със сървър, на който в цифров вид се съхраняват чувствителни в търговско отношение данни, лични данни на служителите и лични данни на клиенти. За да спази правните си задължения за обезопасяване на данните срещу непозволен достъп, работодателят е инсталирал система за контрол на достъпа, която записва влизането и излизането на служители, разполагащи със съответното разрешение да влизат в помещението. Ако изчезне елемент от оборудването или ако данните станат

[18] РГ29, *Становище 05/2014 относно техническите способи за анонимизиране*, WP216, 10 април 2014 г., URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_bg.pdf.

обект на непозволен достъп, загуба или кражба, поддържаните от работодателя записи му позволяват да определи кой е бил в помещението в онзи момент.

Предвид факта, че обработването е необходимо и не надхвърля правото на неприкосновеност на личния живот на служителите, то може да бъде обосновано със законен интерес по силата на член 7, буква е), ако служителите са информирани по подходящ начин относно операцията по обработване. Постоянното наблюдение на честотата и точните моменти на влизане и излизане на служителите обаче не може да бъде оправдано, ако тези данни се използват и за друга цел, например за оценка на работата на служителя.

5.6 Операции по обработване, при които се използват системи за видеонаблюдение

Видеонаблюдението и мониторингът продължават да пораждат същите проблеми за неприкосновеността на личния живот на служителите, както преди — възможността за непрекъснато проследяване на поведението на работника[19]. Най-значимите промени във връзка с използването на тези технологии в контекста на трудово или служебно правоотношение са свързани с възможността за лесно осъществяване на дистанционен достъп до събраните данни (например чрез смартфон); намаляването на размера на камерите (успоредно с увеличаването на техните възможности, например висока разделителна способност); и обработването, което може да се извършва чрез нови инструменти за видеоанализ.

С възможностите, осигурени от инструментите за видеоанализ, работодателят може да наблюдава израженията на работника чрез автоматизирани средства, да открива отклонения от предварително определени модели на движение (например в контекста на завод) и други. Това би било непропорционално по отношение на правата и свободите на служителите, поради което е принципно незаконосъобразно. Обработването също така вероятно би включвало профилиране и евентуално автоматизирано вземане на решения. Поради това работодателите следва да се въздържат от използването на технологии за разпознаване на лица. Възможно е да съществуват някои ограничени изключения от това правило, но тези сценарии не могат да служат за общо легитимиране на използването на такива технологии[20].

5.7 Операции по обработване, които включват превозни средства, използвани от служителите

Широко възприети станаха технологиите, които позволяват на работодателите да наблюдават своите превозни средства, особено при организации, чиито дейности включват превоз или които разполагат със значителен автомобилен парк.

Работодателите, които използват телематични приложения в превозни средства, събират данни както относно превозното средство, така и относно използващия го служител. Тези данни могат да включват не само данни за местонахождението на превозното

[19] Вж. цитираното по-горе решение по дело *Körpke/Германия*; освен това следва също така да се отбележи, че в някои юрисдикции беше постановено за допустимо инсталирането на системи, например вътрешна система за видеонаблюдение с цел доказване на незаконосъобразно поведение; вж. решението по дело *Bershka* от Конституционния съд на Испания.

[20] Освен това съгласно ОРЗД обработването на биометрични данни с цел идентифициране трябва да се основава на едно от изключенията, посочени в член 9, параграф 2.

средство (и съответно на служителя), които се събират от обикновени системи за проследяване с GPS, но в зависимост от технологията могат да включват и друга богата информация, включително поведението при кормуване. Определени технологии също така могат да позволяват непрекъснато наблюдение както на превозното средство, така и на водача (например устройства за записване на данни за събития).

Възможно е работодателят да бъде задължен да инсталира технология за проследяване в превозните средства, за да демонстрира спазването на други правни изисквания, например за да гарантира безопасността на служителите, които ги управляват. Освен това е възможно работодателят да има законен интерес да бъде в състояние да открие местонахождението на превозните средства във всеки един момент. Дори ако работодателите имат законен интерес да постигнат тези цели, първо следва да се оцени дали обработването за тези цели е необходимо, и дали реалното изпълнение отговаря на принципите на пропорционалност и субсидиарност. Когато се позволява използване на служебен автомобил за лични нужди, най-важната мярка, която работодателят може да въведе, за да се гарантира спазването на тези принципи, е да се осигури възможност за отказ: служителят принципно следва да има възможност временно да изключи проследяването на местонахождението, когато специални обстоятелства оправдават това, като например посещение при лекар. По този начин служителят може по своя инициатива да защити определени данни за местонахождението като лични. Работодателят трябва да гарантира, че събраните данни не се използват за по-нататъшно незаконосъобразно обработване, като например проследяване и оценка на служителите.

Работодателят също така трябва ясно да информира служителите, че на управлявания от тях служебния автомобил е инсталирано устройство за проследяване и че техните движения се записват, докато използват превозното средство (включително, в зависимост от използваната технология, че може да се записва и тяхното поведение при кормуване). За предпочитане е тази информация да се показва на ясно място във всеки автомобил, в рамките на зрителното поле на водача.

Възможно е служителите да използват служебни автомобили извън работното време, например за лични нужди, в зависимост от конкретните политики относно използването на тези превозни средства. Предвид чувствителността на данните за местонахождението е малка вероятността да има правно основание за наблюдение на данните за местонахождението на използваните от служителите автомобили извън договореното работно време. Ако обаче съществува такава необходимост, следва да се обмислят мерки, които да бъдат пропорционални на рисковете. Например това би могло да означава, че с цел предпазване срещу кражба на автомобила, местонахождението му не се регистрира извън работно време, освен ако той излезе извън определен радиус, който е достатъчно голям (регион или дори държава). Освен това местонахождението се показва само в неотложен случай — работодателят ще задейства „видимостта“ на местонахождението и ще осъществи достъп до данните, които вече са съхранени в системата, само когато превозното средство излезе извън предварително определения регион.

Както е посочено от РГ29 в *Становище 13/2011 относно услугите за гео-локализиране на интелигентни мобилни устройства*[21]:

„Устройствата за проследяване на превозни средства не представляват устройства за проследяване на персонал. Тяхната функция е да проследяват или наблюдават местоположението на превозните средства, в които са инсталирани. Работодателите не трябва да ги считат за устройства за проследяване или наблюдение на поведението или местоположението на шофьорите или на друг персонал, например чрез изпращане на сигнал за скоростта на превозното средство.“

В допълнение към това, както е посочено от РГ29 в *Становище 5/2005 относно използването на данни за местонахождение с оглед на предоставянето на услуги с добавена стойност*[22]:

„Обработването на данни за местонахождението може да бъде оправдано, когато се извършва като част от наблюдение на превоза на хора или стоки или подобрение на разпределението на ресурси за услуги на отдалечени едно от друго места (например планиране на операции в реално време), или когато се преследва цел, свързана със сигурността на самия служител или на поверените му стоки или превозни средства. От друга страна, работната група счита, че обработването на данни е прекомерно, когато служителите са свободни да организират пътуването си както желаят или когато това се извършва единствено с цел наблюдение на работата на служителя, при условие че може да се наблюдава чрез други средства.“

5.7.1 УСТРОЙСТВА ЗА ЗАПИСВАНЕ НА ДАННИ ЗА СЪБИТИЯ

Устройствата за записване на данни за събития осигуряват на работодателя техническата възможност да обработва значително количество лични данни относно служителите, които управляват служебни автомобили. Такива устройства все по-често се поставят в превозните средства с цел запис на видео, евентуално със звук, в случай на произшествие. Тези системи са в състояние да записват в определени моменти, като реагират например на рязко спиране, рязка промяна в посоката или злополуки, като записват моментите непосредствено преди произшествието, но могат да бъдат настроени за постоянно наблюдение. Тази информация впоследствие може да се използва за наблюдение и преглед на поведението на лицето при кормуване с цел подобряването му. Освен това много от тези системи включват GPS за проследяване на местонахождението на превозното средство в реално време, а за по-нататъшно обработване могат да се съхраняват и други подробности, свързани с кормуването (например скоростта, с която се движи превозното средство).

Тези устройства станаха особено широко разпространени при организации, чиито дейности включват превоз или които разполагат със значителен автомобилен парк. При все това поставянето на устройства за записване на данни от събития може да бъде законно само ако съществува необходимост от обработването на получените по този

[21] РГ29, *Становище 13/2011 относно услугите за гео-локализиране на интелигентни мобилни устройства*, WP185, 16 май 2011 г., URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_bg.pdf.

[22] РГ29, *Становище 5/2005 относно използването на данни за местонахождение с оглед на предоставянето на услуги с добавена стойност*, WP115, 25 ноември 2005 г., URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf.

начин лични данни относно служителя за законна цел и ако обработването отговаря на принципите на пропорционалност и субсидиарност.

Пример

Транспортно дружество оборудва всички свои превозни средства с видеокамера в кабината, която записва видео и звук. Целта на обработването на тези данни е да се подобрят шофьорските умения на служителите. Камерите са настроени да съхраняват записи при определени събития, като например рязко спиране или рязка промяна в посоката. Дружеството приема, че законният му интерес съгласно член 7, буква е) от Директивата да защити безопасността на своите служители и на други водачи представлява правно основание за обработването.

При все това законният интерес на дружеството да наблюдава шофьорите не е с предимство пред правата на тези шофьори за защита на личните им данни. Постоянното наблюдение на служителите с такива камери представлява сериозно вмешателство по отношение на тяхното право на неприкосновеност на личния живот. Съществуват други методи (например поставяне на оборудване, което не позволява използването на мобилни телефони), както и други системи за безопасност, като например усъвършенствана система за аварийно спиране или система за предупреждение при напускане на лентата за движение, които могат да се използват за предотвратяване на пътнотранспортни произшествия и които могат да бъдат по-подходящи. Освен това при такива видеозаписи съществува голяма вероятност да се стигне до обработване на лични данни на трети страни (например пешеходци), а за такова обработване законният интерес на дружеството не е достатъчен, за да бъде обосновано обработването.

5.8 Операции по обработване, включващи разкриване на данни на служителите на трети страни

Предприятията все по-често предават данните на своите служители на клиентите си, с цел да се гарантира надеждно предоставяне на услуги. Тези данни могат да бъдат доста прекомерни в зависимост от обхвата на предоставяните услуги (например могат да включват снимка на служителя). Обаче с оглед на неравнопоставеността в отношенията служителите не са в позиция да изразят свободно своето съгласие за обработването на техните лични данни от работодателя и ако обработването на данни е непропорционално, работодателят не разполага с валидно правно основание.

Пример:

Дружество за доставка изпраща на своите клиенти електронно писмо с връзка към името и местонахождението на куриера (служителя). Дружеството също така възнамерява да предостави паспортна снимка на куриера. То приема, че разполага с валидно правно основание за обработването поради своя законен интерес (член 7, буква е) от Директивата), което позволява на клиента да провери дали куриерът действително е правилното лице.

Обаче не е необходимо на клиентите да се предоставят името и снимката на куриера. Тъй като няма друго законно основание за това обработване, дружеството за доставка няма право да предоставя тези лични данни на клиентите.

5.9 Операции по обработване, включващи международно предаване на данни относно човешките ресурси и други данни, свързани със служителите

Работодателите все по-често използват приложения и услуги, основани на изчисления в облака, например предвидени за боравене с данни относно човешките ресурси, както и онлайн приложения за използване в офиса. Използването на повечето от тези приложения води до международно предаване на данни от и относно служителите. Както бе посочено в Становище 08/2001, член 25 от Директивата гласи, че предаването на лични данни на трета страна извън ЕС може да се извършва само ако тази страна гарантира достатъчна степен на защита. Независимо от основанието, предаването следва да отговаря на разпоредбите на Директивата.

Поради това следва да се гарантира, че разпоредбите относно международното предаване на данни се спазват. РГ29 повторно изтъква изразената преди това позиция, че е за предпочитане да се разчита на подходяща защита, а не на дерогациите, изброени в член 26 от ДЗЛД; когато се разчита на съгласие, то трябва да бъде конкретно, недвусмислено и свободно изразено. Освен това обаче следва да се гарантира, че данните, споделени извън ЕС/ЕИП, и последващият достъп на други субекти в рамките на групата остават ограничени до необходимия за преследваните цели минимум.

6. Заключения и препоръки

6.1 Основни права

Съдържанието на горепосочените съобщения и данните за трафика във връзка с тези съобщения са обхванати от същата защита на основните права като „аналоговите“ съобщения.

Електронните съобщения, направени от служебни помещения, могат да бъдат обхванати от понятията „личен живот“ и „кореспонденция“ по смисъла на член 8, параграф 1 от Европейската конвенция. Въз основа на настоящата Директива за защита на личните данни работодателите могат да събират данни само за законни цели, като обработването трябва да се извършва при подходящи условия (например да бъде пропорционално и необходимо, за действителен и съществуващ интерес, по законен, предварително определен и прозрачен начин) и въз основа на правно основание за обработването на личните данни, събрани от електронни съобщения или генерирани чрез тях.

Фактът, че работодателят притежава електронните средства, не изключва правото на тайна на служителите по отношение на техните съобщения, свързаните с тях данни за местонахождението и кореспонденцията. Проследяването на местонахождението на служителите чрез притежаваните от тях или предоставените от предприятието устройства следва да бъде ограничено до случаите, когато е строго необходимо за законна цел. Ако се прилага принципът „Донеси своето собствено устройство“, естествено е важно служителите да имат възможност да защитят своите лични съобщения от всякакво наблюдение във връзка с работата.

6.2 Съгласие; законен интерес

Служителите почти никога не са в позиция да дават, отказват или отменят свободно своето съгласие с оглед на зависимостта, която възниква в резултат на отношенията работодател/служител. С оглед на неравнопоставеността на силите служителите могат да изразят свободно своето съгласие само в изключителни обстоятелства, когато приемането или отхвърлянето на дадено предложение не е обвързано с никакви последици.

Понякога работодателите могат да се позоват на законния си интерес като правно основание, но само ако обработването е строго необходимо за законна цел и ако отговаря на принципите на пропорционалност и субсидиарност. Преди да бъде въведен инструмент за наблюдение, следва да се извърши проверка за пропорционалност, за да се прецени дали всички данни са необходими, дали това обработване надхвърля общите права на неприкосновеност на личния живот, с които разполагат служителите на работното място, и какви мерки трябва да се предприемат, за да се гарантира, че нарушенията на правото на неприкосновеност на личния живот и правото на тайна на съобщенията са сведени до необходимия минимум.

6.3 Прозрачност

На служителите следва да бъде съобщено по ефективен начин за извършваното наблюдение, целите на това наблюдение и обстоятелствата, както и възможностите на служителите да предотвратят събирането на техни данни от технологиите за наблюдение. Политиките и правилата относно законосъобразното наблюдение трябва да бъдат ясни и лесно достъпни. Работната група препоръчва при създаването и оценката на тези правила и политики да бъде включена и представителна извадка от служителите, тъй като повечето видове наблюдение разполагат с потенциал за вмешателство в личния живот на служителите.

6.4 Пропорционалност и свеждане на данните до минимум

Обработването на данни на работното място трябва да представлява пропорционален отговор на рисковете, пред които е изправен работодателят. Например злоупотребите с интернет могат да бъдат открити, без да е необходимо да се анализира съдържанието на уебсайтовете. Ако злоупотребата може да бъде предотвратена (например чрез използване на уеб филтри), работодателят не разполага с общо право за наблюдение.

Освен това цялостната забрана на съобщения за лични нужди не е практична и прилагането ѝ може да изисква непропорционално равнище на наблюдение. Много по-голямо значение следва да бъде отдадено на предотвратяването, отколкото на разкриването — интересите на работодателя се обслужват по-добре чрез предотвратяване на злоупотребата с интернет с помощта на технически средства, отколкото чрез изразходване на ресурси за откриване на злоупотреби.

Събираната от текущото наблюдение информация, както и информацията, която се показва на работодателя, следва да бъдат сведени до възможния минимум. Служителите следва да разполагат с възможност за временно изключване на проследяването на местонахождението, ако обстоятелствата оправдават това. Могат да се разработят решения, например за проследяване на превозни средства, които регистрират данните за местоположението, без да ги представят на работодателя.

Работодателите трябва да вземат под внимание принципа за свеждане на данните до минимум, когато вземат решение за въвеждането на нови технологии. Информацията следва да се съхранява за минималния необходим период от време, като срокът на задържане е определен. Когато информацията вече не е необходима, тя следва да бъде заличена.

6.5 Услуги с изчисления в облака, онлайн приложения и международно предаване на данни

Когато от служителите се очаква да използват онлайн приложения, които обработват лични данни (като например онлайн офис приложения), работодателите следва да обмислят дали могат да позволят на служителите да посочват определени лични пространства, до които работодателят не може да получава достъп при никакви обстоятелства, като например лична поща или папка за документи.

Използването на повечето видове приложения в облака води до международно предаване на данни на служителите. Следва да се гарантира, че предаването на лични данни към трета държава извън ЕС се извършва само когато е гарантирано подходящо равнище на защита, както и че данните, споделени извън ЕС/ЕИП, и последващият достъп на други субекти в рамките на групата остават ограничени до необходимия за преследваните цели минимум.

* * *

Съставено в Брюксел на 8 юни 2017 г.

За работната група:
Председател
Isabelle FALQUE-PIERROTIN