حریم خصوصی متقاضیان کار و کارگران

*باقر انصاری

چکیده

در همه کشورهای جهان، کارفرمایان پیش از به خدمت گرفتن اشخاص متقاضی کار و گاه پس از استخدام، اطلاعات مختلفی درباره تخصص، وضعیت سلامتی، وضعیت خانوادگی، عادتهای فردی، حسن یا سوء سابقه افراد جمع آوری می کنند. در برخی اماکن کار نیز برای تامین امنیت اشخاص حاضر یا اموال موجود یا برای جلوگیری از نقض قوانین و قواعد کار، با استفاده از فناوریهای مختلف، نظارتهای سمعی و بصری آشکار یا پنهان به صورت موقت یا مستمر صورت می گیرد.

با توجه به امکان ورود کارفرما به حریم خصوصی اشخاص متقاضی کار یا کارگران و نیز به دلیل امکان سوء استفاده کارفرمایان از اطلاعات شخصی و غیر مرتبط با کار اشخاص متقاضی کار یا کارگران، تدابیری برای حمایت از حریم خصوصی این اشخاص لازم است. مقاله حاضر در صدد است ضمن معرفی مصادیق اعمال تهدید کننده حریم خصوصی اشخاص متقاضی کار یا کارگران، برخی از تدابیر بین المللی و ملی را که برای رفع تهدید مذکور، توصیه یا استفاده شده بررسی کند.

بند اول - تأثیر پیشرفت علم بر نقض حریم خصوصی توسط کارفرمایان

در سراسر دنیا کارگران تابع نظارت هایی هستند که از سوی کارفرمایان آنها صورت می گیرد. کارفرمایان، محل کار، روند کار و مسایل مربوط به مستخدمان و کارگران خود به دلایل مختلفی همچون تأمین امنیت اشخاص و اموال موجود در محل کار، رعایت مسایل بهداشتی و ایمنی در محل کار، کنترل کیفیت تولید یا ارایه خدمات، مورد نظارت قرار می دهند و اطلاعات شخصی مستخدمان و کارگران را خود را جمع آوری می کنند.[1]

در سالهای اخیر، در نتیجه تغییر مستمر ساختار و ماهیت محل کار، انجام نظارت های پنهانی و نقض کننده حریم خصوصی مستخدمان و کارگران افزایش یافته است. پیشرفت تکنولوژی، کمیت و کیفیت نظارت های کارفرمایان بر امور کارگران بسیار آسان کرده است. اکنون نظارت بر کار، رفتار و ارتباطات مستخدمان و کارگران با توسل به ابزارهای تکنولوژیکی و با سهولت و سرعت زیاد امکان پذیر است. فناوری معاصر به اندازه‌ای قدرتمند شده است که می تواند تمام ابعاد زندگی کارگران را تحت کنترل کارفرما قرار دهد. برای مثال، برنامه های نرم افزاری می توانند تعداد ضربه هایی را که یک کارمند بر کلیدهای رایانه وارد می کند ثبت کنند؛ تکیه کلام های تلفنی و مقصد مکالمات تلفنی نیز قابل شناسایی شده است؛ دوربین های کوچک و نشانهای هوشمند تشخیص هویت می توانند رفتار، حرکات و حتی علایق و گرایش های فیزیکی (جسمانی) کارگران را تحت نظارت قرار دهند.[2]

امروزه، پیشرفت علم سبب شده است که کارفرمایان در کسب جزیی ترین و خصوصی ترین اطلاعات مستخدمان و کارگران خود نیز موفق باشند. در برخی کشورها، تست های روانشناسی عمومی هوش، انجام کار، شخصیت و درستکاری، مواد مخدر، سلامت جسمانی و عدم پیشینه سوء در محل های کار مورد استفاده قرار می گیرد. همچنین، از زمان کشف DNA ، استفاده از آزمایشهای ژنتیک بسیار زیاد شده است. این تست ها، امکان دسترسی کارفرمایان به درونی ترین جزئیات بدن مستخدمان و کارگران را به منظور پیش بینی استعداد بیماری و پذیرش شرایط پزشکی یا حتی رفتاری آنان میسر ساخته است.

بررسی ها نشان می دهد که در سالهای اخیر، نظارت اتوماتیک بر محل کار نیز رشد فزاینده‌ای داشته است. اکنون سیستم های شبکه‌ای پیشرفته می توانند به طور خودکار، رایانه ها را مورد تفتیش قرار دهند تا احراز کنند که کدام نرم افزار، فعال است و چگونه و به چه روشی کار می کند و چه اطلاعاتی از آن رد و بدل می شود. برنامه های نرم افزاری می توانند

*عضو هیات علمی دانشکده حقوق دانشگاه شهید بهشتی

کنترل تمامی رایانه های شخصی افراد را در اختیار مدیران قرار دهند. اکنون مدیران می توانند از راه دور، برنامه های هر دستگاه را در حالی که مسیر پست الکترونیک و فعالیت اینترنتی آنها را خوانده و مورد تجزیه و تحلیل قرار می دهند تغییر داده یا متوقف کنند.

گزارش اخیری که توسط انجمن مدیریت آمریکا منتشر شده است نشان می دهد که حدوداً هشتاد درصد از شرکتهای بزرگ آمریکایی به هنگام کار، ارتباطات مستخدمان و کارگران خود را از جمله با نظارت بر مکالمات تلفنی، فایل های رایانه ای، پستهای الکترونیک و ارتباطات اینترنتی، مورد کنترل و بازرسی قرار می دهند و یا به قصد ارزیابی چگونگی انجام کار و اهداف امنیتی از نظارتهای ویدیویی استفاده می کنند.[۳]

اکنون هر کارفرمایی می تواند میزان استفاده از یک رایانه را از طریق بررسی تعداد دکمه ها یا کلیدهایی را که توسط یک کارمند داده پرداز از طریق سیستم Word که در یک مدت زمانی خاص وارد شده مورد نظارت قرار داده و مدت زمانی را که رایانه در خلال روز کاری، عاطل و باطل مانده است مشخص کند. ابزارهای نظارت بر کم و کیف کار مستخدمان و کارگران با رایانه ها، در بازار به قیمتهای کم یافت می شود و همین امر باعث شده است که برنامه های تجسس، نه تنها در میان کارفرمایان دستگاههای دولتی شایع شود بلکه بخش خصوصی نیز از این وسایل استفاده کند.[۴]

استفاده از دوربین های ویدیویی و تلویزیون های مدار بسته، روش رایج دیگری جهت نظارت بر کارگران در کارگاه است و بسیاری از حوزه هایی را که کارگران سابقاً در آن حوزه ها از انتظار بالایی نسبت به حریم خصوصی برخوردار بودند نظیر حمام ها و اتاق های رخت کن و استراحت و استخرها تحت نظارت های فزاینده قرار داده است.[۵]

اکنون برخی از بیمارستان های خارجی پرستاران خود را ملزم می سازند تا نشانها و علامتهایی را بر لباسهای متحدالشکل خود نصب کنند. پیشرفتهایی که در این زمینه صورت گرفته به شرکتهای حمل و نقل این امکان را داده تا یک سامانه الکترونیکی را در کامیونها نصب کنند که این سامانه ها موقعیت دقیق وسیله نقلیه را به صورت لحظه لحظه به پایانه اصلی خود گزارش می کند. شرکتهای حمل و نقل با استفاده از این سامانه ها می توانند مطمئن شوند که رانندگان آنها هیچ گونه میسر خارج از برنامه یا انحراف از مسیر پیش بینی شده نداشته اند. چنین سیستمهای در سراسر انگلستان مورد استفاده قرار می گیرد.[۶]

بنابراین، پیشرفت علم و دستیابی به فناوری های نو سبب شده است نظارت بر کارگران و جمع آوری اطلاعات شخصی آنها بیش از پیش آسان و کم هزینه و پنهانی شود. مطابق با آخرین مطالعه ای که "بنیاد حریم خصوصی" آمریکا انجام داده است در عمل، قیمت و هزینه پایین فناوریهای نظارتی است که بیش از هر چیز دیگر به افزایش نظارت بر محل های کار کمک کرده[۷] و در بسیاری از موارد، حریم خصوصی و کرامت کارگران را به طور جدی به مخاطره انداخته است.

پیشرفت علم و دستیابی به فناوری نو سبب شده است، نظارت بر کارگران و جمع آوری اطلاعات شخصی آنها بیش از پیش آسان و کم هزینه و پنهانی شود

بند دوم - سطح انتظار از حریم خصوصی در اماکن کار

الف- مفهوم حریم خصوصی و سطح انتظار از آن

انسانها در زمانها و مکانها و موقعیتهای مختلف زندگی خود انتظارات متفاوتی نسبت به مسایل خصوصی خود دارند. در برخی اوضاع و احوال، مایل نیستند حتی کوچکترین نکته ای از مسایل خصوصی آنها افشا شود و گاهی به آشکار شدن برخی مسایل خصوصی خود رضایت می دهند. بر این اساس، دو ضابطه برای شناسایی مصادیق مشمول این حریم وجود دارد: ضابطه نوعی که به موجب آن، انسان ها نوعا یا عرفاً برخی جنبه های زندگی خود را حریم خصوصی دانسته و لازم نیست توجیه کنند چرا دیگران نباید بدون رضایت آنها به آن جنبه های زندگی دسترسی و اطلاع پیدا کنند. ضابطه شخصی که به موجب آن، انسانها می توانند برخی جنبه های زندگی خود را که نوعا یا عرفاً از شمول حریم خصوصی خارج است جزء مسایل شخصی و داخل در قلمرو حریم خصوصی خود اعلام کنند.

بنابراین، می توان حریم خصوصی را به این صورت تعریف کرد: قلمروی از زندگی هر فرد است که آن فرد نوعاً و عرفاً یا با اعلان قبلی، انتظار دارد دیگران بدون رضایت وی به اطلاعات راجع به آن قلمرو دسترسی نداشته باشند یا به آن قلمرو وارد نشوند یا به آن قلمرو نگاه یا نظارت نکنند و یا به هر صورت دیگری وی را در آن قلمرو مورد تعرض قرار ندهند؛ ورود بدون اجازه به منازل و اماکن خصوصی، ایست و بازرسی های بدنی و تفتیش بدن، رهگیری انواع مکالمات و ارتباطات، دسترسی به اطلاعات شخصی، افشای مسایل خصوصی در جامعه، فضولی در امور دیگران و پاییدن افراد از مهمترین مصادیق اعمال نقض کننده حریم خصوصی محسوب می شوند.

بدینسان، قلمرو حریم خصوصی تا حدود زیادی نسبی و تابع اوضاع و احوال است. اوضاع و احوالی که طبق آنها، "انتظار معقول و متعارف[۸]" از حریم خصوصی در برابر دسترسی و نظارت دیگران پدید می آید و قابل حمایت است.[۹]

این عوامل و اوضاع و احوال عبارتند از:

۱. مکان مورد نظارت

۲. موضوع مورد نظارت

۳. استفاده‌ای که اطلاعات حاصل از نظارت ممکن است داشته باشد
۴. وسایلی که برای نظارت مورد استفاده قرار می گیرد
۵. وضعیت شخصی که مورد نظارت واقع می شود
۶. رضایت
۷. روابط بین طرفین.

۱. مکان مورد نظارت: منزل یا اماکن خصوصی در مقایسه با اماکن عمومی

انسان هنگامی که در منزل یا مکان خصوصی به سر می برد بیشترین انتظار برخورداری از حریم خصوصی را دارد. برعکس، انتظار معقول اشخاص نسبت به حریم خصوصی به هنگامی که آنها در یک مکان عمومی قرار دارند محدود می شود. اشخاصی که در اماکن عمومی به سر می برند باید قبول کنند که آنها تابع و تسلیم حوادث و اتفاقات عادی و طبیعی زندگی اجتماعی روزمره هستند. لذا اخذ تصاویر اتفاقی در یک مکان عمومی عادتاً نباید نقض حریم خصوصی افرادی به شمار رود که تصویرشان به طور اتفاقی و به دلیل حضور آنها در آن مکان در یک زمان خاص گرفته شده است.[۱۰]

قلمرو حریم خصوصی تا حدود زیادی نسبی و تابع اوضاع و احوال است

۲. موضوع مورد نظارت: زندگی عاطفی یا خصوصی در مقایسه با زندگی معمولی و روزمره

"انتظار معقول و متعارف" اشخاص از حریم خصوصی ممکن است با توجه به موضوع مورد نظارت متغیر باشد. نظارت حتی اگر در یک مکان عمومی صورت گیرد به هنگامی که هدف آن جستجو و شکار گوشه‌ها و زوایای خصوصی و عاطفی زندگی یا شخصیت اشخاص باشد و به ویژه شخصی که مورد تعرض نظارتی واقع شده است در زمان نظارت، آسیب پذیر یا ناتوان از دفاع باشد نقض حریم خصوصی محسوب می شود.

۳. استفاده‌ای که اطلاعات حاصل از نظارت ممکن است داشته باشد: انتشار عمدی یا سایر استفاده‌هایی که می تواند موجب صدمه و لطمه به اشخاص شود در مقایسه با استفاده‌های بی ضرر "انتظار معقول و متعارف" از حریم خصوصی به ویژه جایی پدید می آید که به قصد انتشار یا استفاده در زمینه‌ای که ممکن است برای اشخاص زیان بار باشد از افراد تصویربرداری یا فیلم‌برداری شود.[۱۱]

۴. وسایلی که برای نظارت مورد استفاده قرار می گیرد:

چشم غیر مسلح یا استماع طبیعی در مقایسه با تکنولوژی پیشرفته در صورت استفاده از برخی ابزارهای نظارتی پیشرفته، "انتظار معقول و متعارف" نسبت به حریم خصوصی تشدید می شود. یعنی استفاده از تکنولوژی ناقض حریم خصوصی می تواند فعالیت نظارتی‌ای را که در غیر این صورت مجاز می بود، به ویژه در مکان‌های عمومی، غیرمجاز گرداند. این استفاده، علی الخصوص اگر پنهانی و با استفاده از وسایل نظارتی دوربرد نظیر عدسی ها یا میکروفونهای پرقدرت صورت گرفته باشد به احتمال زیاد، نقض حریم خصوصی به شمار خواهد آمد.[۱۲]

همچنین استفاده از تجهیزات سمعی و ویدئویی برای مقاصد لب خوانی و تجسس در مکالمات چه در اماکن خصوصی صورت گیرد و چه در اماکن عمومی، نقض فاحش "انتظار معقول و متعارف" از حریم خصوصی به شمار می رود.[۱۳]

۵. وضعیت شخصی که مورد نظارت واقع می شود: اشخاص عمومی در مقایسه با اشخاص خصوصی

اشخاصی که در انظار مردم قرار دارند به ویژه به هنگامی که با خواست خویش خود را در منظر عمومی قرار داده باشند نظیر سیاست مدارانی که خود را آماده انتخابات می سازند یا هنرمندان و دیگر اشخاص مشهور، نمی توانند یکسان با سایر شهروندان انتظار برخورداری از حریم خصوصی داشته باشند.[۱۴]

با وجود این، در منظر عموم قرار گرفتن سبب نمی شود که آنها به طور مطلق از حمایت های حق حریم خصوصی محروم شوند. حتی اشخاص عمومی نیز در رابطه با جزئیات کاملاً عاطفی زندگی شخصی خود از حق حریم خصوصی برخوردار هستند و این حق را به هنگام ورود به زندگی عمومی از دست نمی دهند.

۶. رضایت: هر نوع فعل قبلی توسط شخصی که مورد نظارت واقع شده دال بر قصد وی به برخورداری از حمایت های حق حریم خصوصی یا عدول جزئی از حق حریم خصوصی اشخاصی که عالماً عامداً اقدام به افشای جنبه‌های زندگی خصوصی خود می کنند با رفتار خود یک انتظار تقلیل یافته از حریم خصوصی ایجاد می کنند. البته، چنین مردمی با انجام آن افعال کاملاً از حق خود نسبت به حریم خصوصی صرف نظر نمی کنند و به دیگران برای ورود بدون اجازه به تمام مسایل زندگی خود چراغ سبز نشان نمی دهند.[۱۵]

۷ - روابط بین طرفین

"انتظار معقول و متعارف" از حریم خصوصی ممکن است بر حسب طبیعت رابطه میان طرفین متغیر باشد. رابطه استخدامی و کاری، زناشویی، ابوت و سایر روابط مشروع می توانند سطح "انتظار متعارف و معقول" حریم خصوصی را تحت تأثیر قرار دهد.[۱۶]

ب - سطح انتظار از حریم خصوصی در محل کار

با توجه به آنچه گفته شد کارگران می توانند در محل کار خود نیز مایل به عدم افشای برخی مسایل خود برای کارفرما یا سایرین باشند. اما توقع برخورداری از حریم خصوصی

در این مکانها (به دلیل عمومی بودن مکان، رضایت کارگر و پذیرش شرایط کار، وجود رابطه کاری و ...) کمتر از انتظاراتی است که آنها می توانند در محل سکونت خود داشته باشند. اماکن کار، شامل اتاق پذیرش، دبیرخانه، اتاق مدیران ارشد، دستشویی ها، رختکن ها، اتاق های مشترک، رستوران، وسایل نقلیه محل کار و دیگر فضاهای باز نظیر پارکینگ اتومبیل ها و عرصه هایی می شود که مشتریان در آنجا به سر می برند. طبیعی است که در هر یک از مکانهای مذکور انتظارات متفاوتی از حریم خصوصی وجود داشته باشد.[۱۷]

برای مثال، در دعوای اوکونر علیه اورتگا[۱۸]، بیمارستانی دولتی، دفتر کار یکی از کارمندان خود را در ارتباط با تحقیقاتی که راجع به یک تخلف گزارش شده انجام می داد مورد تفتیش قرار داد. دادگاه عالی ایالات متحده چنین رأی داد که هر کارگری دارای انتظار معقول از حریم خصوصی است که این انتظار باید در چارچوب رابطه کاری و با توجه به واقعیت های عملیاتی کارگاه تعیین شود که ممکن است انتظارات کارگر را به استناد رویه عملی دفتر یا محل کار و آیین و روشهای مرسوم مردم در آنجا یا از طریق مقررات مشروعی کاهش دهند.[۱۹] به طور کلی، محل کار یک چهار دیواری شخصی نیست که از هرگونه ورود ناظران یا دیگر کارگران و ارباب رجوع مصون باشد. مدیران ارشد یا بازرسان می توانند در صورت غیبت کارگر از محل کارش، به اموال اداری که در دفتر کارگر موجود هستند و یا روی میز کار او قرار دارند دسترسی داشته باشند. همچنین ممکن است آنها به انجام تفتیش هایی جهت کشف تخلفاتی که نسبت به قواعد محل کار یا مقررات دولتی صورت می گیرد نیاز داشته باشند. بنابراین، کارگر، حداقل نسبت به میز کار خود و پرونده های کمد کاری خود در صورتی می تواند انتظار معقول حریم خصوصی داشته باشد که:

۱- میز کاری یا فایل های کمد کاری او مشترک با دیگر کارگران نباشد.

۲- فایلهای کاری او در دفتر محل کارش نگهداری نشوند.

۳- کارفرما هیچگونه مقررات یا خط مشی ای که کارگر را نسبت به نگهداری اقلام شخصی در میز یا فایل های کمد کاری خود بیمناک کند نداشته باشد.

همچنین، در قضیه ک- مارت علیه تروتی[۲۰] کارگران مجاز به استفاده از قفل هایی بودند که توسط کارفرما برای کمدهای آنها در نظر گرفته شده بود. هنگامی که شرکت کارفرما به بازرسی و تفتیش کمدهای کارگران پرداخت، دادگاه حکم به محکومیت این عمل صادر کرد.[۲۱]

بدین ترتیب مشخص می شود که روابط بین کارگر و کارفرما و حل تعارض بین منافعی که از یک سو کارگر در حفظ اطلاعات شخصی خود حتی به هنگام استخدام و پس از آن دارد و نیز منافعی که از داشتن یک کارگاه سالم و کارآمد و مولد عاید کارفرما می شود نیازمند تأمل زیاد است تا تعادل ظریف و دقیق بین این منافع متقابل ایجاد شود.

کارگران معمولاً در حوزه های زیر با نقض حریم خصوصی خود مواجه هستند:[۲۲]

۱- گزینش استخدامی

۲- آزمایش مواد مخدر، الکل، ایدز، آزمایشهای روانشناسی و جنسیت

۳- بازرسی ها و تفتیش های بدنی محسوس و غیر محسوس

۴- نظارت (مانیتورینگ)

۵- افشای اطلاعات خصوصی نظیر اطلاعات پزشکی

۶- ورود کارفرما به مسائل و فعالیت های غیرکاری آنها

پیش از مطالعه هر یک از حوزه های فوق، اشاره به این نکته ضروری است که حمایت از حریم خصوصی کارگران یکی از دغدغه های سازمان بین المللی کار است و این سازمان موازین و اصول خاصی را در این باره تدوین کرده است که به دلیل اهمیت، ذیلاً، به برخی از آنها اشاره می شود.

بند سوم: نگاهی به موازین سازمان بین المللی کار و قوانین سایر کشورها در مورد حریم خصوصی کارگران

الف- موازین سازمان بین المللی کار

همانطور که گفته شد پیشرفت فناوریهای نظارت، شمار نقض حریم خصوصی افراد در محلهای کار را افزایش داده است. امروزه، کارفرمایان می توانند انجام کار، رفتار، گفتار و ارتباطات کارگران خود را با استفاده از روشهای زیر مورد نظارت و بازرسی قرار دهند:

۱- مکالمات تلفنی با ارباب رجوع و مشتریان، قابل رهگیری است. ارتباطات پست یا صدای الکترونیک کارگران نیز قابل نظارت شده است.

۲- داده هایی که در صفحه رایانه ای شبکه رایانه ای شرکت ظاهر ذخیره می شوند توسط کارفرما قابل نظارت است.

۳- سرعت ضربه زدن به کلیدهای رایانه توسط کارگرانی که مشغول کار با برنامه Word هستند از سوی کارفرمایان آنها قابل نظارت است.

۴- کارفرمایان می توانند علملیات اجرایی کارگران را با بررسی میزان وقتی که آنها از طریق رایانه سپری کرده اند مورد نظارت قرار دهند.

۵- حرکت هایی که در محل کار صورت می گیرد از طریق دوربین های ویدیویی قابل مشاهده و ضبط می باشد.[۲۳]

سازمان بین المللی کار اعلام می کند که اقدامات مذکور

در اکتبر ۲۰۰۱، کمیسیونر حریم خصوصی انگلستان پیش نویس قانونی را برای روابط کارفرمایی و کارگری منتشر ساخت

و استفاده از فناوری های نظارت در کارگاهها، نگرانی های زیر را در رابطه با حریم خصوصی کارگران ایجاد کرده است:

"۱-استفاده کارفرمایان از تکنولوژی های نظارت، نقض حقوق بنیادین بشر و شرافت بشری است و غالباً بدون توجه کافی به چنین امری صورت می گیرد.

۲-نظارت بر بانک های داده های رایانه ای، بازشنودهای تلفنی و نظارتهای ویدیویی، فضولی و ورود در زندگی شخصی کارگران را بیش از پیش آسان ساخته و کشف این اقدامات بیش از پیش مشکل می گردد.

۳-بازبینی، بازشنود و نظارت کارفرمایان این احساس را در کارگران ایجاد می کند که قابل اعتماد نیستند و در نتیجه یک روحیه انفعالی در آنها ایجاد می کند که هم برای کارگر و هم برای کارفرما مضر است.

۴-اقدامات فوق ممکن است به صورت تبعیض آمیز یا برای تلافی کردن و انتقام جویی علیه کارگران صورت گیرد". [۲۴]

کارگران می توانند در محل کار خود نیز مایل به عدم افشای برخی مسائل خود برای کارفرما یا سایرین باشند. اما توقع برخورداری از حریم خصوصی در این مکانها کمتر از انتظاراتی است که آنها می توانند در محل سکونت خود داشته باشند

سازمان بین المللی کار برای رفع نگرانیهای مذکور، در قالب یک مجموعه قواعد رفتاری موسوم به "مجموعه قواعد رفتاری سازمان بین المللی کار در حمایت از داده های شخصی کارگران" توصیه هایی را در مورد نحوه نصب وسایل نظارتی، جمع آوری داده ها و نیز نحوه استفاده از داده های جمع آوری شده ارائه کرده است. به موجب بند ۶-۱۴ مجموعه مذکور:

"۱-چنانچه کارگران با نصب مانیتور مورد نظارت قرار گیرند باید از پیش، از دلایل این امر، برنامه زمانی نظارت و روش ها و فنون به کار گرفته شده و از داده هایی را که قرار است جمع آوری شوند آگاه گردند و کارفرما باید ورود به حریم خصوصی کارگران را به حداقل ممکن کاهش دهد.

۲-نصب مانیتورهای نظارتی مخفی تنها در صورتی مجاز است که:

۲-۱-مطابق با قوانین ملی صورت گیرد؛

۲-۲-بر مبنای دلایل معقولی، ظن فعالیت مجرمانه یا دیگر تخلفات شدید در محل کار وجود داشته باشد.

۳-نظارت فوق تنها در صورتی می تواند مستمر باشد که برای بهداشت، امنیت یا حمایت از مالکیت لازم باشد". [۲۵]

گفتنی است که در تدوین مجموعه قواعد رفتاری حمایت از داده های شخصی، اصول و رهنمودهای کلی دفتر بین المللی کار مورد توجه واقع شده است که از جمله می توان به اصول زیر اشاره کرد:

"داده های شخصی باید به صورت قانونی و منصفانه مورد استفاده قرار گیرند. تنها به خاطر دلایلی که مستقیماً به اشتغال کارگر مربوط می شوند و تنها در جهت مقاصد اولیه ای که برای جمع آوری داده ها وجود داشته است می توان از آنها استفاده کرد.

کارفرمایان نمی توانند داده های شخصی حساس (نظیر داده های راجع به زندگی جنسی کارگران، باورهای سیاسی، مذهبی و سایر اعتقادات، عضویت در اتحادیه های کارگری یا محکومیت های کیفری) را جمع آوری کنند مگر آنکه آن اطلاعات مستقیماً به امر استخدام کارگر مرتبط بوده و مطابق با قوانین ملی جمع آوری شده باشد؛

در جمع آوری اطلاعات نباید از تصویرهای چندگانه، تجهیزات حقیقت یاب یا هر نوع روش آزمایش مشابه استفاده شود؛

داده های پزشکی، باید تنها مطابق با قوانین ملی و اصول حاکم بر امور محرمانه پزشکی جمع آوری شود. معاینات ژنتیک باید ممنوع شده یا تنها به مواردی که صریحاً توسط قوانین ملی تجویز شده است محدود شود. آزمایشهای مواد مخدر تنها مطابق با قوانین ملی و استانداردها و رویه بین المللی قابل انجام است؛

کارگران باید پیش از انجام نظارت بر آنها از این امر آگاه شوند و جمع آوری داده ها از طریق چنین نظارتی نمی تواند به عنوان تنها عامل ارزیابی کار مورد استفاده قرار گیرد؛

کارفرمایان باید امنیت اطلاعات شخصی را تضمین کنند و از گم شدن آن اطلاعات، دسترسی های غیر مجاز به آنها یا استفاده غیر قانونی یا تغییر یا افشای آنها جلوگیری کنند. کارگران باید به طور منظم از تمامی داده هایی که کارفرما راجع به آنها نگهداری می کند مطلع گردیده و به آن داده ها دسترسی داشته باشند". [۲۶]

مجموعه اصول مذکور برای کشورها لازم الاتباع نیستند ولی برای کمک به پیشرفت قانونگذاری ها، تدوین مقررات، قراردادهای جمعی کار، اصول و قواعد کار پیش بینی شده اند. با وجود این، متأسفانه قوانین موجود در جهان، از کشوری به کشوری دیگر متفاوت بوده و در برخی کشورها، محدودیت های قانونی بسیار کمتری نسبت به نظارت در محل های کار وجود دارد. برای مثال در ایالات متحده آمریکا، حدود دو سوم از کارفرمایان، ارتباطات و فایل های الکترونیک کارگران خود را حتی بدون اطلاع قبلی مورد بازبینی یا شنود قرار داده اند. تحقیق دیگری که اخیراً توسط بنیاد حریم خصوصی [آمریکا] صورت گرفته نیز نشان می دهد که ۱۴ میلیون کارگر در ایالات متحده، تابع یک نظارت سمعی بصری مستمر هستند که این تعداد در صورتی که نظارت های موردی نیز مورد توجه قرار گیرد بسیار زیاد خواهد شد. کارفرمایان می توانند به نحو موردی یا اتفاقی پیامهای ارسالی پست الکترونیک برخی کارگران را مورد مانیتورینگ (نظارت) قرار دهند و یا کلید واژه هایی را برای نشان دادن پستهای

الکترونیک برگزینند. در صورت اخیر، یک نرم‌افزار می تواند تمام پیامهای ارسالی و دریافتی شرکت از طریق پست الکترونیک را عبارت به عبارت تجزیه و تحلیل کرده و نتایجی را درباره اینکه آیا پیامهای مذکور در راستای امور شرکت بوده است یا نه، ارائه دهد. به این نرم‌افزار می توان دستور داد تا برخی کلیدواژه‌ها را جستجو کند. حتی برخی برنامه‌های نرم‌افزاری می توانند از الگو سیستم‌هایی جهت تجزیه و تحلیل نمونه‌های ارتباطی و تبدیل آنها به تصاویر استفاده کنند.[۲۷]

ب- مطالعه تطبیقی

در کشورهای اروپایی، جمع‌آوری و علنی سازی اطلاعات شخصی، به طور یکنواخت تحت حمایت "دستورالعمل حمایت از داده ها" قرار دارد. با وجود این، "دستورالعمل ۱۹۹۷ ارتباطات از راه‌دور"[۲۸]، محرمانه بودن ارتباطات را تنها برای سیستم‌های عمومی پیش‌بینی می کند و لذا، شامل سیستم‌های متعلق به اشخاص خصوصی در اماکن کار نمی‌شود. علی رغم این امر، بسیاری از کشورهای اروپایی نظیر، استرالیا، آلمان، نروژ و سوئد قوانین محکم کار و مقررات حریم خصوصی تنظیم کرده‌اند که مستقیم یا غیر مستقیم، این نوع از نظارت ها را ممنوع یا محدود می کند. در فنلاند قانون جدید حمایت از داده ها در محیط کار، از اکتبر ۲۰۰۱ لازم‌الاجرا شده است.[۲۹]

در فرانسه به موجب قانون کار، کارگران باید از کاربرد هر گونه وسیله توسط کارفرما برای ضبط اطلاعات شخصی آنها مطلع شوند. طبق ماده ۱۲۷۸ قانون مذکور، اطلاعات شخصی کارگران یا متقاضیان کار را تنها با رضایت آنها می توان جمع آوری کرد. استفاده از نظارت ویدیوئی و سایر وسایل نظارتی تنها تحت شرایط خاص مجاز است. اثبات وجود یک مشکل امنیتی و اخطار به کارگران در مورد کاربرد وسایل نظارتی از جمله این شرایط است. همچنین، طبق رویه قضایی فرانسه استناد به ادله ای که با استفاده از وسایل نظارت پنهانی به دست آمده است برای اثبات تخلف انضباطی غیرقابل پذیرش اعلام شده است. دیوان کشور فرانسه در سال ۲۰۰۱ در یک رأی مشهور اعلام کرد که کارگران حتی در محل کار و در ساعات کار از حق حریم خصوصی برخوردارند و لذا مستحق رعایت محرمانه بودن مکاتبات و مکالمات خود با کارفرمایان هستند. اکنون، کارفرمایان از دسترسی به پست الکترونیک (E-Mail) کارگران خود ممنوع هستند و حتی اگر بتوانند اثبات کنند که پست الکترونیک کارگران آنها محدود و مربوط به امور شغلی آنها می شود تأثیری در این ممنوعیت ندارد.

در اکتبر ۲۰۰۱، کمیسیونر حریم خصوصی انگلستان پیش‌نویس قانونی را برای روابط کارفرمایی و کارگری منتشر ساخت[۳۰]. در مارس ۲۰۰۲، اولین بخش این قانون درباره حمایت از داده ها در جریان استخدام و گزینش کارگران منتشر شد[۳۱]. سه بخش بعدی آن درباره سوابق استخدامی، نظارت در زمان کار و اطلاعات و آزمایشهای پزشکی متعاقباً به مرحله اجرا در خواهد آمد.

در ۱۹۹۹، دولت سوئد کمیته‌ای را مأمور مطالعه مسائل حریم خصوصی در محل های کار نمود. در مارس ۲۰۰۲ کمیته مذکور، طرحی را برای وضع قانون خاصی جهت حمایت از اطلاعات خصوصی کارگران فعلی، کارگران گذشته و متقاضیان کار در بخشهای خصوصی و عمومی ارائه کرد.[۳۲]

در می ۲۰۰۲، "گروه کاری حمایت از داده های مشمول ماده ۲۹ اتحادیه اروپایی" یک گزارش کاری درباره انجام نظارت بر ارتباطات الکترونیک در محل کار منتشر کرد. در این سند فهرستی از سؤالاتی را که پیش از انجام نظارت باید پاسخ داده شوند مطرح شده است[۳۳]. برای مثال، می توان به سؤالات زیر اشاره داشت: آیا فعالیت نظارتی، برای کارگران شفاف و روشن است؟ آیا این امر، ضروری است؟ آیا کارفرما نمی تواند همان نتایج را با استفاده از روشهای سنتی نظارت بدست آورد؟

همچنین در خارج از اروپا نیز تحولاتی در این زمینه صورت گرفته است. در ژوئن ۲۰۰۲ "کمیسیون حمایت از داده های هنگ کنگ"، پیش‌نویس یک قانون درباره محل های عمومی را به مشورت عمومی گذاشت. این پیش‌نویس شامل تلفن، سی‌سی تی‌وی، پست الکترونیک و استفاده از کامپیوتر و نظارت بر محل می‌شد.[۳۴] استرالیا در سال ۲۰۰۰ با تصویب قانون اصلاح حریم خصوصی (بخش خصوصی)، محدودیت های کمتری را درباره نظارت کارفرمایان بر ارتباطات کارگران وضع کرد. زیرا قانون اصلاحی، استفاده از سیاست های رسمی را پیش از انجام نظارت لازم الرعایه اعلام کرد. همچنین طبق قانون مذکور، کارفرمایان باید اثبات کنند که نظارت بر پستهای الکترونیک برای مثال به دلیل استفاده بیش از اندازه از پست الکترونیک، توزیع مطالب موهن، فعالیت های احتمالاً کیفری و یا افشای اطلاعات حساس موجه می‌باشد. با وجود این، شرکتهای کوچک و رسانه‌های همگانی و سوابق کارگران در بخشهای صنعتی از این امر مستثنی هستند.[۳۵]

دادگاه‌های آمریکا، نوعاً در زمینه شناخت حق حریم خصوصی کارگران کند عمل کرده‌اند. در این کشور هیچگونه راه‌حل قانع کننده و متحدالشکلی که سطح حریم خصوصی کارگران و چگونگی حمایت از آنها را نشان دهد وجود ندارد. بسیاری براین باورند که چون کارفرمایان دارای حق مالکیت یا حق کنترل بر اماکن کار،

موجودی و تسهیلات آن اماکن هستند کارگران تمامی حقوق و انتظارات خود نسبت به حریم خصوصی و مصونیت از تعرض در این زمینه را از خود ساقط کرده‌اند. برخی دیگر نیز از پاسخ به مسأله حریم خصوصی کارگران اینگونه طفره می‌روند که اخذ رضایت کارگران نسبت به انجام نظارت و کنترل و آزمایش بر روی آنها به عنوان یکی از شرایط اشتغال، ضروری است. اخیراً، قانونگذار این کشور، کارفرمایان را از انجام برخی گزینش های استخدامی، برخی آزمایشهای حین استخدام یا پس از استخدام، پاییدن‌ها و نظارت های مخفیانه بر ارتباطات و رایانه های کارگران خود منع کرده است.[۳۶]

بند چهارم- نظارت ویدیویی در محل کار

نظارتهای ویدیویی به دلایل متعددی صورت می گیرند. گزارشی که از سوی کمیته حریم خصوصی نیوولز جنوبی درباره این نوع نظارتها منتشر کرده نشان می دهد که عمده‌ترین دلایل نظارتهای ویدیویی کارفرمایان عبارتست از:[۳۷]

۱.جلوگیری از سرقت اموال شرکت توسط کارگران یا مشتریان و کشف این جرم؛

۲.جلوگیری از سرقت اموال کارگران و کشف این جرم؛

۳. جلوگیری از سوء استفاده نسبت به اسرار تجاری شرکت و کشف سوء استفاده ها؛

۴.جلوگیری از عاطل و باطل ماندن دارایی شرکت؛

۵.نظارت بر کیفیت انجام کار توسط کارگران؛

۶.بهبود ارائه خدمت به مشتریان؛

۷.تعلیم کارگران؛

۸.حصول اطمینان از جریان تولید شرکت؛

۹.جلوگیری از انجام خرابکاری و از کار انداختن روند تولید شرکت؛

۱۰.حمایت از سلامت کارگران در قبال خطرات موجود؛

۱۱.حمایت از امنیت کارگران برای مثال در قبال سرقتهای توام با خشونت؛

۱۲.پیشگیری نسبت به احتمال ایجاد مسؤولیت برای آنها در قبال هتک هرمت، نقض کپی رایت، ایذاء و اذیت و تبعیض؛

۱۳.تعیین مسؤولیت کارفرما، کارگر و شخص ثالث در صورت بروز اختلاف.

علیرغم آثار مثبتی که نظارت ویدیویی دارد اما چنانچه نظارت به صورت مستمر انجام شود کارگران را دچار استرس کرده و سبب می شود آنها کار خود را با اضطراب انجام دهند. حتی سبب می شود که برخی رفتارها و فعالیتهای شخصی کارگران نظیر خارش بدن و تنظیم لباس، برای آنها آزار دهنده شود. همچنین ممکن است داده های شخصی حساس کارگران که ارتباط چندانی با کار آنها ندارد نیز جمع آوری شود و سرانجام، اطلاعات ضبط شده به گونه‌ای تفسیر شود یا مورد استفاده قرار گیرد که تصویر غلطی از شخصیت یا عملکرد اجرایی یک کارگر ارائه دهد و برای اعتبار و آینده شغلی او بسیار زیان‌بار باشد.[۳۸]

علاوه بر این، آگاهی کارگران از این امر که مدیر ارشد، رفتار آنها را زیر نظر دارد می تواند مانع حرکتها و ارتباطات آنها شود. چنانچه نظارت (مانیتورینگ) مخفیانه صورت گرفته باشد ولی نهایتاً توسط کارگران کشف شده باشد به شدت روحیه کارگران را تضعیف کرده و جو بی اعتمادی بین کارگران و کارفرمایان ایجاد می کند. خطر دیگر آن است که احتمال دارد کارفرمایان هدف مشروعی برای نظارت ویدئویی داشته باشند اما این امر ممکن است پس از نصب دوربین ها و بدون اطلاع کارگران برای اهداف و مقاصد دیگر نیز مورد استفاده قرار گیرد.[۳۹]

بنابراین، می توان گفت که نظارت ویدیویی کارگران تنها زمانی مجاز است که اطلاعات جمع آوری شده توسط کارفرمایان محدود به کارکارگران باشد. نظارت بر کارگران در اتاق خواب، دستشویی، رختکن و جاهای مشابه عموماً باید ممنوع شود. نظارت ویدیویی باید بر اساس یک هدف مشروع صورت گیرد. کارگران باید از یک فرصت معقول نسبت به مشاهده اطلاعات جمع آوری شده توسط کارفرما برخوردار باشند.[۴۰]

با مطالعه تطبیقی اصول هادی نظارت ویدیویی علنی (غیر پنهانی) می توان اصول زیر را برای انجام نظارت ویدیویی در اماکن کار مورد توجه قرار داد:[۴۱]

۱.انجام نظارت باید برای یک هدف مشروع صورت پذیرد؛

۲.روش های دیگری که کمتر ناقض حریم خصوصی هستند قابل دسترس نباشد؛

۳.کارگران باید از شکل و هدف نظارت در زمانی که داده های آنها جمع آوری می شود و یا در اولین فرصت ممکن پس از آن آگاه شوند؛

۴.نظارت باید به روش غیر مخفیانه صورت گیرد مگر آنکه نفع برتری وجود داشته باشد که استفاده از وسایل مخفی برای جمع آوری داده های شخصی را توجیه کند؛

۵.دوربین ها باید تنها در مکانهایی نصب شوند که در آنجا خطر امنیتی بالایی وجود دارد؛

۶.نظارت در توالتها، دوشهای حمام و اتاقهای رختکن ممنوع است؛

۷.ذخیره کردن داده های شخصی جمع آوری شده از طریق نظارت ویدیویی، حفاظت و استفاده از آنها باید مطابق با اصول حمایت از داده های شخصی باشد.

بند پنجم - نظارت ویدیویی پنهانی در محل کار

نظارت پنهانی بوسیله دوربین های مخفی اصولاً باید

حمایت از حریم خصوصی کارگران یکی از دغدغه های سازمان بین المللی کار است و این سازمان موازین و اصول خاصی را در این باره تدوین کرده است

ممنوع شود مگر آنکه ظن قوی نسبت به انجام فعالیت غیر قانونی در محل کار وجود داشته باشد. کمیسیونر حریم خصوصی مشترک المنافع استرالیا اعلام کرده است که مؤسسات داخل مشترک المنافع باید به هنگام تصمیم گیری نسبت به انجام نظارتهای پنهانی به نکات زیر توجه داشته باشند(این نکات در مورد آژانس های امنیتی که به قصد اجرای قانون نظارت های پنهانی انجام می دهند اعمال نمی شود):[۴۲]

۱.نظارت پنهانی باید تنها برای یک هدف مشروع که در ارتباط با فعالیت مؤسسه می باشد صورت گیرد؛

۲.هر مؤسسه ای باید اوضاع و احوال و شرایط یا تخلفاتی را تعریف کند که به خاطر آنها ممکن است نظارت پنهانی صورت گیرد و اعمالی را که می توانند اعمال نظارت از سوی موسسه را توجیه کنند برشمارند؛

۳.تصویب انجام نظارت پنهانی در هر قضیه خاص باید توسط مدیران ارشد صورت گرفته و روشها و آیین و محل انجام فعالیتهای نظارتی نیز مشخص شود؛

۴. در تصمیم گیری نسبت به انجام نظارت پنهانی، مؤسسات باید معیارها و ضوابط زیر را مورد توجه قرار دهند؛

۴-۱- ظن معقولی وجود داشته باشد که یک تخلف یا فعالیت غیر قانونی در شرف انجام است یا در حال انجام است یا انجام یافته است؛

۴-۲-دیگر اشکال و روش های تحقیقات مورد توجه قرار گرفته و نامناسب تشخیص داده شده اند یا دیگر اشکال تحقیقات مورد آزمایش قرار گرفته و نامناسب یا غیر پاسخگو تشخیص داده شده اند؛

۴-۳-منافع حاصل از کسب اطلاعات مورد نظر از طریق نظارت پنهانی تا حد زیادی نسبت به منافع حریم خصوصی برتری داشته باشد.

کمیته حریم خصوصی نیوولز جنوبی نیز به عنوان نتیجه گزارش خود در مورد نظارتهای ویدیویی پنهانی، این نوع نظارتها را در موارد زیر قابل توجیه دانسته است:[۴۳]

۱.یک مشکل خاص و جدی امنیتی وجود داشته باشد؛

۲.کارفرما درباره منبع فعالیت غیر قانونی مظنون باشد؛

۳.دیگر تدابیر امنیتی، ناکارآمد تشخیص داده شده باشند؛

بند ششم- تحقیقات استخدامی کارفرمایان در مورد کارگران

کارفرما نیاز دارد تا درباره فعالیت کارگران خود در حین کار اطلاعاتی داشته باشند تا هم از مسؤولیت هایی که بی احتیاطی و بی مبالاتی کارگران متوجه او می سازد جلوگیری کند و هم یک کارگاه سالم و کارآمد و مولد داشته باشد. به همین منظور، کارفرمایان غالباً خود را مکلف می دانند و گاهی نیز قانون آنها را ملزم می سازد تحقیقاتی در مورد برخی جنبه های زندگی شخصی و کاری کارگران خود به عمل آورند.

این تحقیقات که معمولاً با حریم خصوصی کارکنان تعارض پیدا می کند در حوزه های زیر صورت می گیرد:

۱. کشف حسن یا سوء سابقه
۲. آزمایش اعتیاد به مواد مخدر یا الکل
۳. رعایت یا نقض مقررات ایمنی
۴. سرقت یا تخریب اموال کارگاه
۵. نقض مقررات اخلاقی و قواعد حرفه ای کار
۶. رفتارهای خلاف قانون کارگران
۷. صلاحیت و شایستگی کارگران.[۴۴]

برخی از تحقیقات کارفرما پیش از استخدام کارگران صورت می گیرد و برخی پس از استخدام. چنانچه کارفرما در انجام هر یک از تحقیقات مذکور مرتکب تقصیر شود و بویژه کوتاهی کند ممکن است در قبال اقدامات کارکنان خود مسؤول شناخته شود. از سوی دیگر، وسواس کارفرما در انجام تحقیقات ممکن است به نقض حریم خصوصی کارگران منجر شود.

در فرانسه به موجب قانون کار، کارگران باید از کاربرد هرگونه وسیله توسط کارفرما برای ضبط اطلاعات شخصی آنها مطلع شوند

غالباً اطلاعاتی که زمان گزینش استخدامی کسب می شود عبارت است از:

۱. اطلاعات راجع به تخصص متقاضی
۲. اطلاعات راجع به شهرت و اعتبار متقاضی
۳. اطلاعات راجع به تواناییهای ذهنی و جسمی متقاضی
۴. سابقه محکومیت کیفری متقاضی

برخی معتقدند کارفرمایان باید قبل از جمع آوری اطلاعات راجع به اعتبار و شهرت متقاضیان استخدامی، رضایت آنها را نسبت به انجام تحقیقات کسب کنند و از اطلاعات جمع آوری شده نیز صرفاً برای مقاصد استخدامی استفاده کنند.[۴۵] در واقع، داده های راجع به اعتبار و شهرت افراد در زمره داده های شخصی محسوب می شود. بند الف، ماده ۲ دستورالعمل اروپایی حمایت از داده های شخصی اعلام می دارد که:

"داده های شخصی عبارت است از هرگونه اطلاعات راجع به یک شخص با هویت مشخص یا قابل شناسایی. شخص قابل شناسایی کسی است که به طور مستقیم یا غیرمستقیم، به ویژه از طریق مراجعه به یک شماره تشخیص هویت یا یک یا چند عامل یا فاکتور خاص درباره هویت جسمانی، روانی، ذهنی، اقتصادی، فرهنگی یا اجتماعی قابل شناسایی است".

ماده۶ دستورالعمل اروپایی هماهنگ با اصول و رهنمودهای دفتر بین المللی کار در مورد استفاده از داده های شخصی پیش بینی کرده است که:

"۱- دولت های عضو باید در مورد داده های شخصی

مقرر کنند که:

الف- به طور منصفانه و قانونی به جریان انداخته شوند[۴۶]؛

ب- برای مقاصد خاص، صریح و مشروع جمع آوری شوند و به طریق دیگری که با اهداف مذکور ناسازگار است آنها را به جریان نیندازند. به جریان انداختن داده ها برای مقاصد تاریخی، آماری یا علمی به شرط رعایت پاره‌ای حمایتهای متناسب بلااشکال است؛

ج. در رابطه با مقاصدی که به خاطر آنها، داده‌ها را جمع آوری یا به جریان می اندازند مناسبت و مربوط بودن را رعایت کنند و از حدود آنها تجاوز نکنند؛

د. داده‌ها را به طور صحیح و در صورت لزوم به روز نگهداری کنند. کلیه اقدامات معقول جهت تضمین حذف یا اصلاح داده های غلط یا ناقص با توجه به مقاصدی که به خاطر آنها جمع آوری شده یا به جریان افتاده‌اند، بردارند؛

هـ. داده ها را به شکلی نگهداری کنند که تشخیص هویت شخصی را که داده به او مربوط می شود برای مدتی بیش از آنچه در راستای هدف جمع آوری یا به جریان انداختن آنها لازم است اجازه ندهد. کشورهای عضو باید تضمینات کافی برای داده های شخصی ای که برای مدت های طولانی جهت استفاده های تاریخی، آماری یا علمی نگهداری می شوند مقرر دارند...".

کارفرمایان برای کسب اطلاعات مورد نظر خود ممکن است از انواع آزمایشها استفاده می کنند که قواعد مختلفی بر هر یک از انواع آزمایشها حاکم است. برخی آزمایشها با حریم خصوصی در تعارض جدی هستند و برخی دیگر تعارض چندانی ندارند.[۴۷] در حقوق آمریکا کارفرمایان بخش خصوصی از انجام آزمایشهای زیر ممنوع هستند:

۱- ملزم ساختن انجام آزمایش دروغ سنج یا تقاضای انجام آزمایش مذکور یا تحریک کارفرما جهت انجام آزمایش مذکور

۲- استفاده از نتایج آزمایشهای دروغ سنج یا انجام تحقیق بر روی آنها

۳- اتخاذ هرگونه اقدام مخالف علیه کارمند یا متقاضی استخدام بر مبنای نتایج حاصل از آزمایش دروغ سنج و یا به دلیل امتناع کارمند یا متقاضی استخدام برای تن دادن به آزمایش دروغ سنج.[۴۸]

برخی کارفرمایان از آزمایشهای روان شناختی یا صداقت برای احراز صلاحیت متقاضیان استخدام استفاده می کنند. این آزمایشها، نوعاً متضمن پاسخ سریع به سوالاتی است که برای ارزیابی گرایش ها و علایق متقاضی استخدام طراحی شده است. برخی از دادگاه های آمریکا چنین آزمایشهایی را نقض حریم خصوصی کارگران دانسته‌اند و برخی دیگر، انجام این آزمایشها را صرفاً محدود کرده‌اند.

سازمان بین المللی کار در قالب یک مجموعه قواعد رفتاری موسوم به "مجموعه قواعد رفتاری سازمان بین المللی کار در حمایت از داده‌های شخصی کارگران" توصیه هایی را در مورد نحوه نصب وسایل نظارتی، جمع آوری داده ها و نیز نحوه استفاده از داده های جمع آوری شده ارائه کرده است

کارفرمایان ممکن است از متقاضیان استخدامی یا کارکنان بخواهند که آزمایش اعتیاد انجام دهند. کارفرمایان آزمایشهای مواد مخدر را غالباً به هنگام استخدام و در مورد برخی مشاغل، در دوره های متناوبی از ایام اشتغال انجام می دهند حتی اگر هیچ گونه دلیلی نسبت به سوء رفتار، ضعف عملکرد اجرایی کارگران خود نداشته باشند و یا دلیل دیگری که استفاده از مواد مخدر را مورد ظن قرار دهد موجود نباشد. هزاران وسیله و اسباب کار وجود دارد که می تواند آثار استعمال مواد مخدر را در چند لحظه و حتی بدون مراجعه به هر آزمایشگاهی نشان دهد. این وسایل که به وفور در بازارهای امروزه در دسترس می باشند آزمایشهای مواد مخدر را با بررسی نمونه هایی از مو و یا ادرار مورد تجزیه و تحلیل قرار می دهند تا آثار استفاده از آمفی تامین، ماری جوانا، کوکائین، تریاک و غیره را کشف کنند.[۴۹]

در برخی از قوانین ایالات های آمریکا پیش بینی شده است که کارفرما باید اطلاعاتی را که راجع به وضعیت سلامت کارگران خود به دست می آورد محرمانه نگهداری کند که اطلاعات راجع به اعتیاد یا الکلیسم نیز در زمره اطلاعات قابل حمایت می باشد.[۵۰] آزمایشهای پزشکی نیز باید کاملاً به آزمایش تواناییها و شرایط و ویژگیهای مرتبط با کار متقاضی کار یا کارگر محدود شوند. به دیگر سخن، کارفرما می تواند پیش از استخدام، بررسی های پزشکی لازم را تنها برای احراز توانایی متقاضی استخدام نسبت به انجام برخی وظایف ضروری شغلی انجام دهد.[۵۱]

در برخی کشورها، ملزم ساختن کارمندان بخش عمومی به انجام آزمایش ایدز یا افشای وضعیت جسمی خود از لحاظ ابتلا یا عدم ابتلا به ایدز ممنوع است. با وجود این، انجام آزمایش ایدز پس از استخدام، ممنوع نیست. لکن کارفرما تنها در صورتی اجازه دارد به فعالیت عادی کارگران مبتلا به ایدز خود خاتمه دهند که بیماری آنها تهدید مستقیم بر سلامت و بهداشت دیگران داشته باشد. برای مثال، محل کار او جایی باشد که احتمال رد و بدل مایعات بدنی در آنجا وجود دارد.[۵۲] در واقع، منافع کارفرمایان را در مقابل نگرانی هایی که کارگران یا کارمندان نسبت به حریم خصوصی خود دارند متعادل شده و تنها در صورتی که منافع جامعه نسبت به افشای وضعیت بهداشتی اشخاص بر منافع شخصی آنها نسبت به عدم افشا، غلبه داشته باشد انجام آزمایشهای مذکور و افشای اطلاعات آنها مجاز شناخته شده است.

سر انجام آنکه، در برخی کشورها، استفاده از آزمایشهای ژنتیک و اطلاعات مرتبط با ژنتیک نیز به عنوان معیاری جهت تمایز قایل شدن بین متقاضیان کار یا

کارگران ممنوع است و کارفرمایان نمی‌توانند از کارگران خود بخواهند که به انجام چنین آزمایشی تن در دهند.[۵۳]

بند هفتم - حریم خصوصی ارتباطات شفاهی و تلفنی کارگران

کارگران حق دارند بدون مداخله غیر قانونی و خود سرانه کارفرمایان به تبادل اطلاعات و فعالیتهای ارتباطاتی بپردازند. نظارت (مانیتورینگ) بر ارتباطات کارگران در صورتی خود سرانه نیست که با رضایت صریح یا ضمنی کارگران صورت گیرد. برخی معتقدند به دلیل آنکه فعالیت‌های کارگران طبق قرارداد کار، تحت نظر کارفرما قرار دارد و علی الاصول، کارفرما نسبت به ارتباطاتی که کارگران با استفاده از تجهیزات تهیه شده توسط او صورت می‌دهند دسترسی دارد فرض بر آنست که کارگران از حق حریم خصوصی خود تا حدی اعراض کرده و یا به نقض آن رضایت داده‌اند.[۵۴]

امروزه در کشورهای توسعه یافته، نظارت تلفنی چه در بخش دولتی و چه در بخش خصوصی فراگیر شده است. در ایالات متحده، کارفرمایان برای کنترل تلفن های کارگران در زمینه مقاصد تجاری، اختیار بیشتری دارند. شرکتها در سطح گسترده ای از فن آوری آنالیز تلفن استفاده می کنند.[۵۵] همچنین، کارگران مرکز تلفن تله کام انگلستان[۵۶] با یک برگه آنالیز جامع معرفی می شوند که میزان انجام کار آنها را در مقایسه با دیگر کارگران نشان می دهد. منشی های رزرو خطوط پرواز در ایالات متحده و سایر جاها، گوشی های تلفنی بر سر می گذارند که طول مدت و محتوای تمامی مکالمات تلفنی و نیز مدت استراحت و صرف نهار آنها را مورد کنترل قرار می دهد. در یک قضیه، مکالمات تلفنی دریافت شده بوسیله مأموران رزرو کننده خطوط پرواز به صورت الکترونیک بر مبنای ثانیه به ثانیه مورد نظارت واقع شده بود. مأموران خطوط پرواز، تنها یازده ثانیه بین هر مکالمه فرصت داشتند و حق استراحت آنها در طول روز مجموعاً ۱۲ دقیقه تعیین شده بود. مأموران خط پرواز از این امر شکایت کردند که چرا به آنها بر مبنای اینکه چه اندازه نام مشتریان را در خلال یک مکالمه استفاده می کنند یا بر مبنای اینکه تا چه اندازه جهت غلبه بر اعتراضات اولیه مشتریان نسبت به خرید یک بلیط تلاش می کنند حقوق پرداخت می شود.[۵۷]

در قضیه دیگری، کارفرما به استناد قانون شنود (از راه وصل کردن سیم مخفی) ایالات متحده به کارگران خود اطلاع داده بود که مکالمات تلفنی و شخصی آنها را تنها تا آن اندازه مورد باز شنود یا بازبینی (مانیتورینگ) قرار خواهد داد که برای احراز کاری و شغلی بودن مکالمات ضرورت داشته باشد. دادگاه آمریکا رأی داد که کارگران تنها به بازشنود مکالمات کاری و شغلی خود رضایت داده‌اند و نه به مکالمات شخصی. به اعتقاد دادگاه مذکور، رضایت کارگران به شنود مکالمات آنها مقید به زمانی است که کارگر واقعاً بداند یا باید بداند که یک خط و مشی بازشنود دائم مکالمات در کارگاه وجود دارد و یا کارگر با یک خط تلفنی که صریحاً به مکالمات تلفنی تجاری یا شغلی اختصاص داده شده است یک مکالمه شخصی انجام دهد.[۵۸]

بنابراین، برخی از مکالمات تلفنی کارگران هر چند که در کارگاه صورت گرفته باشند مورد حمایت هستند و کارگران حق دارند تا نسبت به مکالمات شفاهی خود در فضاهای اختصاص داده شده یا محدود شده به آنها نظیر اتاقهای استراحت یا توالت، انتظار حریم خصوصی داشته باشند.

بند هشتم - حریم خصوصی ارتباطات الکترونیکی کارگران

الف. نگرانی های موجود

کارفرمایان می توانند با استفاده از "نرم‌افزار مدیریت اینترنت"[۵۹] که اینترنت و کاربریهای آن را مورد تجزیه و تحلیل قرار می دهد ارتباطات الکترونیکی کارگران را مورد نظارت (مانیتورینگ) قرار دهند. اکنون این امکان برای کارفرمایان وجود دارد که وب سایت‌ها و گروه‌های چتی را(chat) که کارگران آنها مشاهده کرده‌اند مورد بازبینی یا بازشنود قرار دهند. یک بررسی اجمالی که توسط مرکز مدیریت منابع انسانی در ایالات متحده صورت گرفت نشان داد که ۳۶٪ از پاسخ دهندگان (کارفرمایان)، پستهای الکترونیک کارگران را مورد بازبینی و باز شنود قرار می دهند.[۶۰]

بررسی دیگری که توسط Macworld صورت گرفت نشان داد که حدود دو سوم از کارفرمایان، ارتباطات و فایل های الکترونیک کارگران خود را حتی بدون اطلاع قبلی مورد بازبینی یا بازشنود قرار داده‌اند.[۶۱]

تحقیق دیگری که اخیراً توسط بنیاد حریم خصوصی آمریکا صورت گرفته نیز نشان می دهد که ۱۴ میلیون کارگر در ایالات متحده، تابع نظارت سمعی و بصری مستمر کارفرمایان هستند که این تعداد در صورتی که نظارت های موردی نیز مورد توجه قرار گیرد بسیار زیاد خواهد شد. کارفرمایان می توانند به صورت موردی پیامهای پست الکترونیک برخی کارگران را مورد نظارت (مانیتورینگ) قرار دهند یا با یک نرم‌افزار تمام پیامهایارسالی و دریافتی شرکت از طریق پست الکترونیک را که عبارت به عبارت تجزیه و تحلیل کرده

و نتایجی را درباره اینکه آیا یک پیام در راستای امور شرکت بوده است یا نه، ارائه دهد.[۶۲]

دلایلی که کارفرمایان برای نظارت الکترونیکی بر کارگران ارائه می دهند عبارتند از:[۶۳]

۱- بررسی ارتباطات شغلی یا حرفه‌ای از طریق پست الکترونیک؛

۲- جلوگیری از مزاحمت‌های on Line نسبت به پرسنل زیر فرمان خود؛

۳- جلوگیری از اینکه منابع شرکت برای مقاصد عمدتاً شخصی مورد استفاده قرار گیرند؛

۴- جلوگیری از اینکه شرکت آنها به دلیل نقض کپی رایت مسؤول شناخته شود؛

۵- جلوگیری از اینکه شرکت آنها به دلیل هتک حرمت تحت تعقیب قرار گیرد؛

۶- کسب اطمینان از اینکه اسرار تجاری شرکت حفظ شده و افشاء نمی‌شوند.

۷- جلوگیری از انباشته شدن حجم زیاد پستهای الکترونیکی در شبکه‌های ارتباطی شرکت که منجر به مسدود شدن شبکه می‌شود.[۶۴]

۸- جلوگیری از وقت‌کشی کارگران[۶۵]

به گفته مرکز مطالعات مدیریت آمریکا، نزدیک به دو سوم تمام شرکتها، کارگران خود را به خاطر سوء استفاده از پستهای الکترونیکی یا ارتباط اینترنتی، مورد مجازات های انضباطی قرار داده و ۲۷ درصد شرکتها کارگران خود را به خاطر دلایل مذکور اخراج کرده‌اند. برای مثال، در سال ۲۰۰۰ شرکت Dow Chemical، پس از آنکه مطالب موهن و ناخوشایندی در پست الکترونیک کارگران پیدا کرد پنجاه درصد آنها را توبیخ و دویست کارگر را به تعلیق از کار تهدید کرد. این شرکت، پستهای الکترونیک شخصی بیش از هفت هزار کارگر را باز کرد و مورد بررسی قرار داد. به همین طریق در سال ۱۹۹۹، نیویورک تایمز، ۲۳ کارمند خود را به دلیل ارسال پیامهای خلاف عفت مورد توبیخ قرار داد.[۶۶]

نظارت بر اتاقهای چت نیز نگرانی های زیادی را در محل های کار ایجاد کرده است. در میان کارفرمایان تجاری، تمایل فزاینده‌ای نسبت به اخراج یا مورد تعقیب قرار دادن کارگرانی که اسرار تجاری کارفرمارا افشا می کنند یا در اتاق چت خود، نسبت به کارفرما مرتکب هتک حرمت می شوند وجود دارد. بسیاری از مردم به صورت بی‌نام و ناشناس وارد اتاقهای چت می شوند و همین که کارفرما مشاهده می کند بخش معینی از اتاق چت، مشغول یک بیان یا ارتباط نامشروع است به مرکز خدمات صفحه پیام نظیر Yahoo یا America Online اظهارنامه ارسال می کند تا هویت ایجاد کننده پیام را احراز کنند. ارائه دهندگان خدمات نیز اغلب از شناسایی اطلاعاتی که از طریق اظهارنامه رسمی ارسال شده و اشاره به فرد خاص دارد روی گردان هستند. شمار اینگونه دعاوی به سرعت در حال افزایش است و نه تنها حریم خصوصی کارگران را بلکه حق آنها نسبت به گمنام بودن و نیز حق بیان آزاد را تهدید می کند.

بنابراین می توان حریم خصوصی را به این صورت تعریف کرد: قلمروی از زندگی فرد است که آن فرد انتظار دارد دیگران بدون رضایت وی به اطلاعات راجع به آن قلمرو دسترسی نداشته باشند یا ناظر آن قلمرو نشوند یا به هر نحو دیگروی را در آن قلمرو مورد تعرض قرار ندهند

ب - سطح انتظار از حریم خصوصی در ارتباطات الکترونیکی

با توجه به اینکه کارگران در اکثر شرکتها و مؤسسات دولتی یا غیر دولتی، رایانه‌هایی را در اختیار دارند که می توانند به اینترنت وصل شوند آنها بیش از پیش از این امکان برخوردارند که از تسهیلات شرکت یا مؤسسه محل خدمت برای برقراری ارتباطات شخصی استفاده کنند. لذا پرسش این است که آیا کارگران نسبت به انواع ارتباطات الکترونیک خود از انتظار حریم خصوصی برخوردارند؟

در پاسخ به این پرسش باید به محیط کاری و مقررات قانونی و قراردادی حاکم در آن توجه کرد که می تواند سطح حریم خصوصی مورد استحقاق کارگران در آن محیط را تعیین می کنند. به طور معمول، کارگران جهت دسترسی به پیامهای پست الکترونیک خود، کلمه عبور ایجاد می کنند. یک کلمه عبور خصوصی می تواند مؤید این استدلال باشد که پیامهای پست الکترونیک کارگر خصوصی می باشد بویژه، اگر کارگران از این امر آگاه باشند که کارفرمای آنها توانایی نقض کلمه عبور آنها و دسترسی به پستهای الکترونیک آنها را دارد. علاوه براین، اگر پیامهای پست الکترونیک، دارای رمز باشند یا به گونه‌ای کدبندی شده باشند که تنها فرستنده و گیرنده آنها قادر به خواندن آنها باشد می توان گفت که انتظار برخورداری از حریم خصوصی بیشتر است. در غیاب یک خط مشی ای که بیان کند پیام ها خصوصی نیستند یا بیان کند که کارفرما حق دسترسی به پستهای الکترونیک را علی رغم وجود کلمه های عبور شخصی دارد احتمال اینکه دادگاهها، کارگر را نسبت به پیامهای پست الکترونیک خود برخوردار از انتظار متعارف نسبت به حریم خصوصی بشناسد زیاد است.[۶۷]

دادگاههای آمریکا اعلام کرده‌اند که کارگران عموماً نسبت به پستهای الکترونیکی خود از انتظار حریم خصوصی برخوردار نیستند و کارفرمایان می توانند پیامهای دریافتی در سیستم رایانه‌ای خود

را حتی در صورتی که آن پیام‌ها برای کارگران ارسال شده باشند بخوانند. بویژه در فرضی که سیستم پست الکترونیکی متعلق به کارفرماست و کارگران توافق کرده‌اند که از رایانه‌های محل کار تنها در امور کاری استفاده کنند استدلال مذکور، بیش از پیش پذیرفته می‌شود.[۶۸]

برای مثال، در دعوای بورک علیه شرکت نیسان موتور،[۶۹] دادگاه اعلام کرد گرچه خواهان (کارگر) به دلیل داشتن کلمه عبور جهت دسترسی به سیستم و نیز مسؤولیت در قبال حفظ کلمه عبور می‌تواند نسبت به پست الکترونیک خود انتظار حریم خصوصی داشته باشد ولی، به دلیل توافق با کارفرما در مورد استفاده از پست الکترونیک برای اهداف شغلی و حرفه‌ای شرکت، از این انتظار خود نسبت حریم خصوصی اعراض کرده است. او آگاه بود که پستهای الکترونیکش مورد بازبینی و نظارت کارفرما و دیگر کارگران همکارش قرار می‌گیرد.[۷۰]

همچنین در دعوای اسمیت علیه پیلسبوری،[۷۱] کارگری پیامهای موهن و تهدیدآمیز نسبت مدیریت شرکت به مدیر ارشد خود ارسال کرده بود. مدیران شرکت، پس از خواندن پیامهای مذکور، تمامی پیامهای پست الکترونیک کارگران خود را خواندند. کارگران ادعا کردند که رهگیری پیامهای آنها ورود به خلوت و تنهایی آنها و نقض حریم خصوصی محسوب می‌شود. دادگاه چنین رأی داد که در ارتباطات از طریق پست الکترونیک که نسبت به مدیر ارشد و در یک سیستم پست الکترونیک و فراگیر شرکت صورت گرفته است انتظار معقول از حریم خصوصی وجود ندارد حتی اگر شرکت قبلاً به کارگران اطمینان داده باشد که چنین ارتباطاتی رهگیری نخواهد شد. دادگاه تصریح کرد که منافع شرکت در جلوگیری از برداشتها و تفسیرهای نامتناسب و غیرحرفه‌ای و یا حتی جلوگیری از فعالیتهای غیر قانونی در سیستم پست الکترونیک آن، در مقایسه با حق حریم خصوصی، از ارزش بیشتر برخوردار بوده و بر حق اخیر حکومت دارد.[۷۲]

با وجود این، کارفرما حتی در صورتی مجاز به نظارت بر (مانیتورینگ) سیستم‌های رایانه‌ای مورد استفاده کارگران باشد ملزم است این نظارت را مطابق با اصول حمایت از داده‌ها و به جهت مقاصد معقول حرفه‌ای یا شغلی و پس از اطلاع قبلی به کارگران انجام دهد و استفاده او از اطلاعات به دست آمده، با انتظارات معقول کارگران هماهنگ باشد. هنگامی که سیستم پست الکترونیک، امکان مشخص ساختن برخی پیامها را به عنوان پیامهای شخصی فراهم می‌آورد پیامهای کارگران باید محرمانه نگهداری شده و کارفرمایان حق رهگیری آنها را جز در صورت رضایت کارگران نداشته باشد. این امر اهمیت بسیار زیادی دارد که کارگران بدانند چه زمانی و چه چیزی تحت نظارت (مانیتورینگ) قرار گرفته و با اطلاعات حاصله چه خواهد شد.

بدین ترتیب به نظر می‌رسد که بهتر است کارفرمایان، اصول و خط مشی‌های حاکم بر دسترسی به پستهای الکترونیک و استفاده از آنها یا افشای پیامهای ارسالی یا دریافتی کارگران در سیستم‌های ارتباطاتی کارگاه را تدوین کنند. این خط ومشی نامه باید میان انتظارات معقول کارگران از حریم خصوصی خود و منافع مشروع حرفه‌ای و تجاری کارفرمایان، تعادل و توازن ایجاد کند. برای ایجاد چنین تعادلی به نظر می‌رسد که توجه کارفرمایان به اصول زیر ضروری باشد:

"۱. خط مشی‌ها و اصولی را برای بیان انتظارات کارگران نسبت به حریم خصوصی خود تهیه کنند؛

۲. میزان نظارت مانیتورینگ را تعیین کرده و نظارت مذکور را محدود به فعالیت‌های مرتبط با کار یا مدیریت بنمایند. میزان نظارت (مانیتورینگ) باید در خط مشی‌های شرکت مورد تصریح قرار گیرد؛

۳. به کارگران و مدیریت نحوه اجرای خط مشی‌ها را آموزش داده و این کار را به صورت ادواری تکرار کنند؛

۴. هنگامیکه کارگران به شبکه رایانه‌ای متصل می‌شوند به آنها اخطار داده و این امر را به تأیید آنها برسانند که صفحات رایانه‌ای آنها توسط کارفرما خوانده می‌شود. این اخطار باید صریحاً بیان کند که سیستم و پست الکترونیک جنبه شخصی و خصوصی ندارد؛

۵. حفاظت از پستهای (نامه‌های) ذخیره شده و بازگرداندن آنها را مورد توجه قرار دهند؛

۶. بیان کنند که اطلاعات قابل دسترس چگونه مورد استفاده قرار خواهد گرفت".[۷۳]

منابع و توضیحات :

۱-EPIC Work Place Page: at : "www.epic. org / privacy/ workplace"

۲- Privacy and Human Rights ۲۰۰۲: Electronic Privacy Information Center and Privacy international first edition ۲۰۰۲ ,Printed in the United States of America, p. ۸۶.

۳- Ibid., p. ۹۰.

۴- Ibid.

۵- The American Civil Liberties Union:Workplace Right, Electronic Monitoring, at: "htpp:/www.aclu.org/library/ pbrw.html".

۶- The Privacy Foundation: "The Extent of Systematic Monitoring of Employee Email",

۷- K-Mart v. Trotti: Ibid: N. ۷-۵۵.

۸- Reasonable expectation of Privacy

۹- The Law Reform Commission of Ireland:Report on Privacy: Surveillanceand the Interception ofCommunications, ۱۹۹۸,para. ۲-۹.

۱۰- Ibid., para. ۲-۱۳.

۱۱- Ibid., para. ۲-۱۵.

۱۲- Ibid., para. ۲-۱۶.

۱۳- Ibid.

۱۴- Ibid., para. ۲-۱۷.

۱۵- Ibid ., para. ۲-۱۸.

۱۶- Ibid., para. ۲-۱۹.

۱۷- LRCH, Civil Liability for Invasion of Privacy, ۱۹۹۹, p.۸۴. at: http:/www.info.gov.hk.

۱۸- OConnor v Ortega at:http://www.oyez.org/oyez/resource /case/۲۸۶/.

۱۹- Denise k. Drake and Neely Fedde:Employment Rights and Responsibilities relating to Privacy in the Workplace, p. ۵, at:http:/www.bna.com /bnabooks/ababna/annual / ۲۰۰۷ drake.doc.

۲۰- K-Mart v. Trotti: op.cit., para. ۷-۵۵.

۲۱- Ibid ., para. ۷-۵۵.

۲۲- Victorian Law Reform Commission:Workplace Privacy, Issues Paper p.۲۷, ۲۰۰۲, available at: http:/www.lawreform. vic.gov.au.

۲۳- Ibid., para. ۷-۵۶.

۲۴-International Labour Organization: "Monitoring and Surveillance in workplace", in Conditions of Worked Diget (Vol. ۲۱, Para. ۱, ۱۹۹۳), p. ۲۰.

۲۵- International Labour OrganizationsCodeofPractice on the Protection of Workers Personal Data .An ILO Code of Practice, available at:http:www./ Lo.org/public/english/protection/safework/cops/ english/download/e۰۰۰۱۱.pdf.

۲۶- Ibid.

۲۷- Denise K. Drake and Neely Fedde: op.cit., p. ۱۲.

۲۸- Directive Concerning the Proceedingof Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive ۹۷/۶۶/EC of the European Parliament and of the Council of ۱۵ December ۱۹۹۷), Available at: "http: www۲. echo. lu/legal/en/dataprot/ protection. htm".

۲۹- Privacy and Human Right ۲۰۰۲: op.cit at:"http:/www.dataprotection. Jov.uk/dpr/dpdoc.nsf".

۳۰- Data Commissioner, Employment: available

۳۱- Data Commissioner,Employment:Part ۱:Recruitment Selection,Employment Practices,Data ProtectionCode, available at:http: /www.ccta.gov. uk/dpr/dpdoc.nsf-۲۵-۰۵/۹۹.

۳۲- Summary of the Proposal: available at:"http:/naring. /regeringen.sepropositioner -mm/ sou/ dpf/ sou "۲۰۰۲ - ۱۸a.pdf".

۳۳- Article ۲۹ Data Protection Working Party:Working Ducument on the Survillance of Electronic Communications in the Workplace, available at: "htti :/europa.eu.int/ comm /internal/market/en/ dataprot/ wpdos/wp۵۵-en.pdf ۷.

۳۴- Privacy Commissioner for Personal Data: Draft Code of Pratcice on Monitoring and Personal Data Privacy at Work: Availableat: ;http: www.pco.org.hk/ english/ ordinace / codes.html".

۳۵- Privacy Amendment (Private Sector) Act ۲۰۰۲.

۳۶- Privacy and Human Rights ۲۰۰۲: op.cit., p.۸.

۳۷- The Privacy Committee of New SouthWales:The Report on Video Surveillance in the Workplace, Available at: "http:www.austlii.edu.au/au/other/privacy/video/ index.html".

۳۸- LRCH: Civil Liability for Invasion of Privacy: op.cit., Para. ۷-۷۲.

۳۹- Ibid.

۴۰- Ibid., Para. ۷-۷۳.

۴۱- The Privacy Committee of New South Wales: op.cit., ۱: Guidelines on Overt Video Survillance in the Workplace. Appendix

۴۲- Commonwealth Privacy Commissioner of Australia: Guidelines on Covert Surveillance in Commonwealth Administration, ۱۹۹۲, available at:http:/privacy.gov.au/ publications/covertsurveillance.doc.

۴۳- The Privacy Committee of New South Wales: op.cit., ۴.۳.

۴۴- Denise k. Drake and Neely Fedde : op.cit., p.۶.

۴۵- Denise k. Drake and Neely Fedde : op.cit., p.۷.

۴۶- ماده ۲ دستورالعمل اروپایی حمایت از داده‌های "به جریان انداختن داده‌های شخصی عبارت است از هر نوع عملیات یا مجموعه‌ای از عملیات که بر روی داده‌های شخصی صورت می‌گیرد، خواه با استفاده از وسایل اتوماتیک باشد و خواه بدون استفاده از آنها، نظیر جمع‌آوری، ثبت، سازماندهی، ذخیره، تطبیق یا تغییر، بازیافت، مشاهده، استفاده، افشا از طریق ارسال، اشاعه و ابراز داده‌ها، در اختیار قرار دادن داده‌ها به انحاء دیگر، تنظیم یا ترکیب داده‌ها، بلوکه کردن داده‌ها، حذف یا از بین بردن آنها".

۴۷- Victorian Law Reform Commission: op.cit.,N.۳.۲۱ and seq.

۴۸- Employee Polygraph Protection Act (" EPPA "), Title ۲۹ of U.S. Code, Chapter ۲۲, ۲۰۰۱-۲۰۰۹, available at:http://www.fas.org/sgp/othergov/polygraph/eppa.html.

۴۹- Privacy and Human Rights ۲۰۰۲: op.cit., p.۹۳.

۵۰- Denise K. Drake and Neely Fedde : op.cit., p.۸.

۵۱- Ibid., p.۹.

۵۲- Leckelt v. Board .of Comm rs of Hosp.at: http:/ www.ncbi.nlm.nih.gov/entrez/query.fcgicmd=Retrievedb =PubMedlistuids=۲۲۸۵۰۵۲dopt=Abstract

۵۳- Denise K. Drake and Neely Fedde : op.cit., p.۱۰.

۵۴- LRCH: op.cit., Para. ۷-۶۰.

۵۵- Denise K. Drake and Weely Fedde: op.cit., p.۲۱.

۵۶- British Telecom

۵۷- Privacy and Human Rights: op.cit., p.۹۱.

۵۸- LRCH: op.cit., p.۷-۶۱.

۵۹- Internet Management Software

۶۰- LRCH: op.cit., Para. ۷-۶۳.

۶۱- Ibid.

۶۲- Privacy and Human Rights ۲۰۰۲: op.cit., p.۹۲.

۶۳- LRCH: op.cit., Para. ۷-۶۴.

۶۴- Privacy and Human Rights ۲۰۰۲: op.cit., p.۹۲.

۶۵- Ibid.

۶۶- Ibid., p.۹۳.

۶۷- LRCH: op.cit., Para. ۷-۶۸.

۶۸- LRCH: op.cit., Para. ۷-۶۵.

۶۹- Bourke v Nissan Motor Corporation:at:http:/www. smbtrials.com/recent-publications. full.htm.

۷۰- LRCH: op.cit., Para. ۷-۶۶.

۷۱- Smyth v the Pillsbury

۷۲- LRCH: op.cit., Para. ۷-۶۷.

۷۳- The Law Reform Commission s Report on Privacy: Regulating the Interception of Communications: op.cti., Para. ۴-۸۶.