LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche

GIOVANNI ZICCARDI
Università degli Studi di Milano

vol. 2, no. 1, 2016

ISSN: 2421-2695

LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico giuridiche.

GIOVANNI ZICCARDI
Università degli Studi di Milano
giovanni.ziccardi@unimi,it

ABSTRACT

The evolution of the technological control of the workers is closely related to the improvement of technological tools. From an unsophisticated control mode, targeting the environment and operated through videocameras, the actual framework consists in embedded control tools strictly related to the technologies that are given to the workers for their daily activity.

Thanks to software installed on network servers, mobile phones, tablets and computers, it is possibile now to operate a full control activity which do not distinguish, in most cases, between control over the data related to the employment contract and control over the personal data of the subject and over his private life. This article will address, from a legal informatics point of view, the most common tools to operate such controls

Keywords: Control; Spyware; Embedded tools; Interception; Privacy; GPS

Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche.

SOMMARIO: 1. L'ontologia del controllo nell'era tecnologica: da Orwell a Kafka. – 2. L'incorporazione degli strumenti di controllo nella tecnologia. – 3. Gli strumenti di geo-localizzazione e le tecnologie come microspie. – 4. Le concrete possibilità di controllo tramite le tecnologie. – 5. Controllo occulto, controllo indiscriminato e pervasività dei controlli. – 6. Considerazioni conclusive: i problemi all'orizzonte.

1. L'ontologia del controllo nell'era tecnologica: da Orwell a Kafka.

Il controllo, attraverso strumenti tecnologici, dell'essere umano in generale, e del lavoratore sul posto di lavoro – o fuori dei locali dell'azienda – in particolare, è sempre stato strettamente connesso all'evoluzione tecnologica.

Negli anni settanta e ottanta l'attenzione era volta, soprattutto, nei confronti degli apparecchi telefonici aziendali, delle autovetture di servizio e di ciò che si svolgeva all'interno degli ambienti dell'azienda, ad esempio allestendo pareti di vetro trasparenti, finestre o telecamere.

Il sistema di controllo era "classico", in puro stile orwelliano: un centro che controlla in tempo reale, grazie a telecamere, sovente posizionate in luoghi segreti per consentire una sorveglianza occulta. Accanto alla tecnologia, ben di più poteva la tecnica tradizionale, ossia l'uso di schedari compilati grazie a informazioni provenienti, in quegli anni, soprattutto dalle fonti presso le parrocchie e le questure. La vita lavorativa, comprese le posizioni sindacali e le opinioni politiche del sorvegliato, si controllava tramite le prime tecnologie; la vita privata, tranne casi eccezionali, si controllava raccogliendo informazioni e compilando dossier e schedari.

Lo Statuto dei Lavoratori cercò, *in primis*, proprio di evitare questi fenomeni di controllo occulto che erano visti, allora, come la modalità più invasiva e subdola esistente.

Verso la fine degli anni novanta l'attenzione si è spostata sempre di più verso le telecamere, che non riprendevano più soltanto in tempo reale ma iniziarono a consentire la memorizzazione dei dati anche per lunghi periodi, e che furono subito regolamentate all'interno della normativa sulla protezione dei dati: pur lasciando salve le disposizioni dello Statuto dei Lavoratori, la legge sulla privacy decise di mettere parola in tale settore, prevedendo una disciplina rigorosa volta, sempre, a rendere *evidenti* tali controlli.

Successivamente vi è stato l'avvento dei telefoni cellulari mobili, capaci di scattare fotografie o di effettuare riprese anche all'insaputa del soggetto. Queste nuove tecnologie hanno aperto l'era moderna con l'avvento della rete, dei droni, dei dispositivi aziendali, dei software spia, dei telefoni attivabili da remoto (capaci, quindi, di mettere in discussione anche l'intoccabile principio dell'orario della prestazione lavorativa), degli strumenti GPS posizionabili sulla vettura aziendale addosso al lavoratore.

Si è così disegnato un quadro che permette un raggio di controlli, oggi, mai sperimentato in precedenza.

Ciò ha cambiato completamente l'ontologia del controllo.

Da un metodo orwelliano, pericoloso ma abbastanza semplice da prevedere e contrastare (si trattava dell'evoluzione del tipico "occhio che guarda"), si è passati a un controllo di tipo kafkiano, estremamente frammentato, complesso, labirintico, oscuro e burocratizzato, composto da dati che si incrociano – lavorativi e privati – e da problemi tecnici difficilmente comprensibili per il lavoratore, da catene di responsabilità (l'amministratore di sistema quale cardine o, comunque, le posizioni di potere di chi vanta maggiori competenze informatiche quale nuovo fenomeno di potere) e da una separazione tra vita privata e vita lavorativa ormai inesistente (le tecnologie hanno eliminato tali aspetti).

Il controllo odierno, tramite le tecnologie, è diventato decentralizzato e capillare (vedremo che spesso parte dagli stessi dispositivi addosso al lavoratore), complesso da comprendere, tecnicamente avanzato e, molto spesso, indiscriminato.

2. L'incorporazione degli strumenti di controllo nella tecnologia.

Spesso è la stessa architettura tecnologica a incorporare i due aspetti del controllo e della sorveglianza discussi poco sopra. Internet ha consentito la più ampia diffusione e distribuzione del pensiero ma, allo stesso tempo, si è rivelata perfetto strumento di controllo.

I droni sono l'esempio classico di evoluzione preoccupante del concetto di telecamera. Già le telecamere tradizionali e le web-cam si sono rivelate, da tempo, potenti strumenti di controllo: il drone può, silenziosamente, seguire l'obiettivo e anche colpirlo, vero e proprio occhio incorporato in un sistema tecnologico. Il GPS, dal canto suo, è già presente sui telefoni, sui tablet e sui computer, permette di localizzare la posizione ed è diventato strumento di grande diffusione. I metadati che si riferiscono ai contenuti di documenti, fotografie e video,

consentono di ottenere informazioni aggiuntive controllando, per certi versi, l'utente *dall'interno* del dato digitale.

Sono essenzialmente due le tipologie di controllo che possono essere inserite all'interno delle tecnologie, intendendo quali *tecnologie* sia i dispositivi sia le applicazioni che li fanno funzionare. Le prime sono *volontarie*, ossia il produttore scientemente inserisce caratteristiche votate al controllo all'interno di una tecnologia pensata per un utilizzo fondamentalmente generico. Le seconde sono involontarie, ossia sono funzioni che permettono un controllo, attivabili o meno *dall'utente* e dipendenti dal suo modo di utilizzarle e dalla sua consapevolezza.

Esempio del primo tipo sono i dispositivi inseriti nelle automobili per effettuare l'assistenza da remoto, i dispositivi GPS che tracciano gli spostamenti di veicoli aziendali, alcuni chip o codici correlati ai telefoni cellulari, gli RFID inseriti in capi di abbigliamento o nei badge, righe di codice che comunicano con la casa produttrice via Internet alcune informazioni sul computer del soggetto. Nel secondo tipo rientrano, invece, dispositivi che non sono pensati per il controllo ma contengono hardware o funzioni che permettono un'attività in tal senso, sia se attivate volontariamente dall'utente sia se attivate da remoto a sua insaputa. Si pensi agli strumenti GPS contenuti ormai in ogni strumento mobile, alle web-cam, alle *app* che segnalano automaticamente il luogo dove ci si trova, ai metadati contenuti nei documenti, e così via.

Questi due metodi, oggi, convivono nelle tecnologie più sofisticate che sono disponibili e hanno aggiunto una prospettiva personal, ossia accompagnano la vita del lavoratore in ogni suo momento.

Da tempo si sostiene, in un quadro simile, che una tecnologia per essere sicura nel senso appena trattato, ossia priva di funzioni di controllo, debba essere *trasparente*. Quando si affronta il tema del controllo *dentro* le tecnologie, tale aspetto diventa fondamentale perché presuppone che le tecnologie di controllo possano essere *nascoste*, ossia operare senza la possibilità che il lavoratore ne venga a conoscenza.

Il termine *trasparente* in senso informatico può assumere diversi significati, ma tutti si riferiscono a un concetto cardine: il codice alla base del sistema operativo/software/applicazione e le specifiche delle tecnologie utilizzate debbono essere *conoscibili*. Non è detto che siano conosciute, a volte sono troppo complesse per il non esperto che non è in grado, ad esempio, di leggere o riprogrammare il codice, ma la pubblicità garantisce che qualcuno nel mondo possa verificare il loro funzionamento.

Il non conoscere il codice non permette di comprendere se vi siano funzioni nascoste o meno. La sicurezza tramite *apertura* si scontra con le teorie di

chi difende, invece, la sicurezza tramite il segreto, ossia il tenere nascoste le informazioni. Dal punto di vista del lavoratore sorvegliato e controllato, che è ciò che interessa in questa sede, la trasparenza del codice e della tecnologia è tutto. Il lavoratore deve conoscere, nei dettagli, che potenzialità di controllo, e che dati trattano, le tecnologie usate nei suoi confronti.

3. Gli strumenti di geo-localizzazione e le tecnologie come microspie.

Il primo dispositivo di controllo più comune incorporato oggi in computer, smartphone e tablet è il GPS, o sistema di geo-localizzazione. Si tratta di una tecnologia che serve per controllare la posizione e gli spostamenti di un dispositivo tramite una combinazione di dati provenienti da satelliti. Se il dispositivo è addosso alla persona o a un veicolo, sono seguiti e tracciati anche la persona e il veicolo. Gli usi positivi di tale tecnologia sono tanti: si pensi alla comodità del navigatore e della possibilità di ricerca di luoghi, o al controllo di dispositivi rubati o smarriti. Al contempo, però, possono diventare perfetti strumenti di controllo.

Le informazioni di localizzazione sono in grado, poi, di incorporare in fotografie, video, aggiornamenti di profili su Facebook o Twitter indicazioni sulla posizione dell'utente e, quindi, estendono anche ad altri tipi di dati tale informazione. Ciò è utile se il soggetto ne è consapevole, mentre può comportare una violazione della privacy se il soggetto non è cosciente del fatto che tali informazioni siano inserite nelle sue immagini e rese pubbliche.

Oggi la geo-localizzazione, in termini di precisione, non si basa più solamente su dati provenienti da satellite ma anche su un dialogo con le reti che ci circondano, sia telefoniche sia Wi-Fi, che hanno anch'esse una sorta di *riconoscibilità geografica*. È, quindi, diventato uno strumento con molti volti.

Il tema della geo-localizzazione, accanto alle questioni tecniche sopra esposte, pone aspetti giuridici molto attuali che interessano gli studiosi (1). In Francia, ad esempio, con la legge n. 2014-372 del 28 marzo 2014, è stata emanata una disciplina specifica per le attività di geo-localizzazione svolte nel corso d'indagini giudiziarie. Ricorda Costanzo come, in tale contesto giuridico, la geo-localizzazione sia definita quale l'attività (e il conseguente risultato) dell'applicazione di tecnologie capaci di determinare, con un sempre più trascurabile margine di approssimazione, l'ubicazione nello spazio di un oggetto o di una persona principalmente attraverso un sistema di posizionamento satellitare,

(1) Vedi P. Costanzo, *Note preliminari sullo statuto giuridico della geolocalizzazione (a margine di recenti sviluppi giurisprudenziali e legislativi)*, *Diritto dell'Informazione e dell'Informatica*, 2014, 3, 331.

o mediante la rete cellulare. Tale sistema riguarda oggi anche le comunicazioni telematiche, l'e-banking e le applicazioni di tipo social (2).

Il costituzionalista ricorda, poi, come se ne sia occupata anche la Corte di Strasburgo nella decisione *Uzun c. Repubblica Federale Tedesca*, adita da un cittadino tedesco sospettato di terrorismo che era stato proprio controllato con un GPS installato nella sua vettura. Si discusse alacremente sul punto della base legale e delle garanzie giurisdizionali, ma la misura fu ritenuta *proporzionata*; si riconobbe, però, *l'immensa potenza* di un tale mezzo di sorveglianza, capace di porre una persona sotto un processo di osservazione totale del suo agire e si ritenne inammissibile, comunque, l'ipotesi di sorveglianza totale (3).

In Francia la giurisprudenza era abbastanza concorde nel ritenere la geo-localizzazione, simile alla sorveglianza *de visu* e ai pedinamenti e da omologarsi, quindi, a semplici atti investigativi privi di lesività per la vita privata e il segreto epistolare, anche in quanto realizzata senza atti di coercizione. Per la Cassazione francese, al contrario, tale tipo di attività costituisce un'ingerenza nella vita privata talmente grave da dover essere sottoposta al vaglio di un giudice. In Italia ci sono alcuni provvedimenti del Garante che si basano sulla qualità dei dati trattati e sulle necessarie informative, oltre alla possibile violazione dello Statuto dei Lavoratori (4).

Negli Stati Uniti d'America il caso *United States vs. Jones* ha visto la Corte Suprema interessata alla valutazione della costituzionalità dell'installazione di un sistema GPS nell'autovettura di un soggetto coinvolto in attività di traffico di droga, evidenziando un'incoerenza rispetto al disposto del Quarto Emendamento e una violazione della ragionevole aspettativa di privacy dell'individuo (5).

In Italia il Garante per la protezione dei dati personali è intervenuto al fine di valutare la conformità alla normativa di un sistema di tracciamento dei dipendenti tramite lo smartphone e il GPS integrato effettuato da diverse compagnie di telecomunicazioni (6).

---

(2) *Ibidem.*

(3) *Ibidem.*

(4) *Ibidem.*

(5) *Ibidem.*

(6) Vedi, ad esempio, "Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Wind Telecomunicazioni s.p.a. - 9 ottobre 2014", in Registro dei provvedimenti n. 448 del 9 ottobre 2014, <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3505371> e "Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a. - 11 settembre 2014", in Registro dei provvedimenti n. 401 dell'11

Il caso è interessante: una società si voleva avvalere di un'innovativa soluzione che prevedeva l'utilizzo di tecniche di geo-localizzazione del dispositivo mobile in dotazione ai circa 900 dipendenti che avevano la qualifica di "tecnico di rete operante sul territorio" e che identificava l'ID del dispositivo aziendale affidato al tecnico, il numero di telefono aziendale, le coordinate GPS del tecnico durante lo svolgimento dell'attività operativa e le coordinate GPS della *home base* del tecnico per la determinazione dell'area di competenza.

Gli scopi erano il miglioramento dei livelli di servizio, assicurando una pianificazione ottimizzata del lavoro, il supporto della gestione delle attività d'emergenza mediante la conoscenza della posizione dei tecnici e l'identificazione del tecnico più qualificato e più vicino al sito per il quale è richiesto l'intervento e il supporto delle misure di sicurezza a tutela dei tecnici coinvolti in attività di servizio allocate in aree remote o disagiate. La società ha, poi, dichiarato che i dati relativi alla posizione geografica dei dipendenti non sarebbero stati utilizzati per finalità *diverse* da quelle rappresentate né potranno essere usati per qualsivoglia fine *disciplinare*.

Circa il potere del dipendente sullo smartphone di controllo, l'invio della posizione geografica del dispositivo non era continuativa ma periodica, con una frequenza di rilevamento dei dati configurabile, il dipendente poteva abilitare o disabilitare la *app* all'inizio e alla fine del servizio, così come durante il servizio stesso, qualora risultasse necessario per esigenze personali, compatibilmente con le procedure aziendali in essere, la piattaforma gestiva l'informazione relativa all'ultima posizione inviata dal dispositivo mobile del tecnico, cancellando quella immediatamente precedente e l'ultima rilevazione veniva cancellata nel momento in cui fosse terminata la sua giornata lavorativa. Il sistema, infine, non eseguiva alcuna storicizzazione del dato di geo-localizzazione, impedendo sia una visione continuativa della posizione del singolo tecnico sia un'eventuale ricostruzione dei relativi percorsi.

Per il Garante tale sistema è ammissibile, ma con garanzie precise da stabilire. In particolare, considerate le potenzialità dei dispostivi smartphone e, segnatamente, la possibilità di raccogliere per loro tramite, anche accidentalmente, informazioni relative alla *vita privata* del dipendente, la società avrebbe dovuto adottare specifiche misure idonee a garantire che le informazioni presenti sul dispositivo mobile visibili o utilizzabili dall'applicazione installata fossero riferibili esclusivamente a dati di geo-localizzazione nonché a impedire l'eventuale

settembre 2014, <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3474069>.

trattamento di dati ultronei quali, ad esempio, i dati relativi al traffico telefonico, agli SMS, alla posta elettronica o altro. Un secondo passo sarebbe stato quello di configurare il sistema in modo tale che sul dispositivo fosse posizionata un'icona che indicasse la funzionalità di localizzazione come attiva; l'icona dovrebbe essere sempre chiaramente visibile sullo schermo del dispositivo, anche quando l'applicazione lavora in background; in applicazione del principio di correttezza del Codice della privacy i trattamenti in esame dovrebbero essere resi noti agli interessati, i quali dovrebbero essere posti nella condizione di conoscere chiaramente finalità e modalità del trattamento.

Una tecnologia, in una seconda ipotesi differente dalla precedente ma altrettanto invasiva, può poi essere surrettiziamente trasformata in *microspia*, solitamente alterando il codice, il sistema operativo o compromettendo l'hardware. Si possono riscontrare due tipi di software che operano in tal senso.
Il primo è comunemente acquistabile in Internet e permette di trasformare il telefono del soggetto preso di mira in una microspia e, quindi, di poter tenere sotto controllo ogni attività.

Vengono, di solito, presentati come prodotti per tenere sotto controllo le attività di minori in famiglia o dei dipendenti sul posto di lavoro ma sono molto più di frequente utilizzati, in realtà, nell'ambito di operazioni di *spionaggio* tra adulti, di cyberstalking e di cyberbullismo. È sufficiente che il soggetto malintenzionato entri in possesso per pochi minuti del telefono da controllare, installi tale programma e, successivamente, sarà in grado, da un pannello di controllo, di leggere i messaggi, vedere le fotografie scattate o custodite, ascoltare le conversazioni in entrata e in uscita, leggere i testi delle comunicazioni in chat di WhatsApp, l'attività in Internet e tante altre informazioni. Si è in presenza di attività illecite in violazione della privacy ed estremamente invasive che, però, sono difficilmente individuabili dal proprietario del telefono. Nel caso il telefono sia consegnato come telefono aziendale dal datore di lavoro al dipendente, occorre che sia chiarito prima dell'utilizzo se il telefono contenga microspie o meno.

Un secondo metodo per utilizzare le tecnologie altrui come microspie è attraverso l'uso di *trojan*, sia da parte di privati sia a opera delle forze dell'ordine o della magistratura per effettuare indagini all'interno di computer. L'uso di strumenti simili è comune anche da parte dell'autorità in alcuni Paesi per prendere di mira telefoni cellulari o computer di giornalisti e dissidenti.

Mentre i software reperibili su Internet sono noti nelle loro funzioni, questi secondi strumenti sono meno conosciuti e si hanno notizie contraddittorie sulla

loro natura e sul loro potenziale; vi è, contemporaneamente, un vivace dibattito circa il loro utilizzo.

L'uso di tali ritrovati apre un dibattito molto interessante che si orienta verso due direzioni: le regole procedurali e il loro rispetto, soprattutto in ambito penalistico e di diritto del lavoro, e l'approccio etico, ossia la consapevolezza dell'utilizzo che verrà fatto di tali strumenti da parte degli acquirenti (in questo caso: il datore di lavoro).

Circa il primo punto, i problemi più spinosi riguardano l'inquadramento corretto di tale fattispecie nuova, il grado della sua invasività e la possibilità di aggirare i mezzi tipici di ricerca della fonte di prova e le loro garanzie soprattutto per l'indagato.

Circa il secondo punto, ci si domanda se sia necessaria una verifica accurata, da parte del venditore di uno strumento così potente, dell'utilizzo che ne farà l'acquirente e, soprattutto, se sarà solo lui a utilizzarlo. Il timore che tali software non siano utilizzati solo nei limiti di legge, ma che se ne possa fare abuso, è, infatti, fondato.

4. Le concrete possibilità di controllo tramite le tecnologie.

Per portare ordine, da un punto di vista informatico, circa modalità possibili di controllo – senza preoccuparsi, per ora, se tali controlli siano contro la legge o ammessi – e muovendo dalla premessa che grazie alle tecnologie è possibile controllare ogni attività, ben più delle telecamere o delle cimici ambientali, è opportuno separare e individuare con cura le seguenti ipotesi:

a) controllo sul dispositivo mobile aziendale fornito al lavoratore. In questo caso ci riferiamo a tutti quei controlli che possono essere effettuati, manualmente o automaticamente, *in loco* o da remoto, su un dispositivo fornito a un lavoratore. Si pensi a un telefono cellulare, a un tablet, a un BlackBerry, a un computer portatile. Più lo strumento è sofisticato, più aumentano le possibilità di controllo del lavoratore da parte del datore di lavoro. In molti casi, il dispositivo è "preparato" e programmato dal datore di lavoro e dai suoi tecnici e fornito al lavoratore, cui non sono lasciate possibilità di disattivazione degli strumenti di controllo o di modifiche ulteriori al dispositivo (ad esempio: per cancellare alcune tracce). Il rischio che questo dispositivo diventi di uso *promiscuo* è alto, anche se in alcuni settori (ad esempio nel settore assicurativo, con tablet utilizzati per la firma grafometrica al fine di concludere contratti in maniera dematerializzata) viene domandato esplicitamente un uso del dispositivo unicamente lavorativo, anche per motivi di sicurezza. Una volta che il telefono, il tablet o il computer portatile è

in mano al datore di lavoro per un controllo, o viene restituito all'azienda, solitamente sono recuperabili *tutte* le informazioni: messaggi scambiati e ricevuti, e-mail, cronologia dei siti visitati, dati cancellati e facilmente recuperabili, fotografie e video.

b) controllo sulle attività di rete di un dispositivo fisso o mobile. Ci si riferisce alla possibilità di tenere sotto controllo e consultare non tanto il singolo dispositivo e i suoi contenuti ma, in maniera più dinamica, ogni attività (in entrata e in uscita) effettuata dal telefono, dal computer o dal tablet riferibile al lavoratore e connessa in rete: siti web visitati, tempo di connessione alla rete, presenza sui social network, file scaricati, attività di messaggistica istantanea.

c) controllo del traffico che è trasmesso *dentro* l'ambiente di lavoro, ossia *sniffing* di pacchetti di dati (ad esempio di comunicazioni via cellulare) o interferenza delle comunicazioni stesse (*jamming*) per impedire l'uso di determinati strumenti in ambiente di lavoro. Lo *snffing* è un procedimento di controllo più sofisticato dei primi due e che consiste nell'installare delle apparecchiature che acquisiscono i pacchetti di dati che circolano nell'etere, quasi sempre in chiaro (ossia facilmente leggibili) e li interpretano. Il *jamming* è, invece, una modalità non di controllo dell'informazione in senso attivo (recuperandola) ma in senso distruttivo, impedendo le connessioni. È di solito usato in ambienti dove, ad esempio, non si vuole che sia presente un segnale di connessione per i cellulari. Il controllo del traffico (in generale) è molto subdolo perché assolutamente neutro per il controllato (non si accorge di nulla, e non subisce rallentamenti nel suo operato informatico). Questo tipo di controllo è indiscriminato, ossia acquisisce sia dati provenienti dai dispositivi mobili personali, sia da quelli lavorativi.

d) controllo utilizzando strumenti spia, quali Remote Access Tools (RAT) o strumenti che replicano le attività del desktop su computer terzi, droni, telecamere evolute o trasformando la webcam in microspia, o il microfono in cimice. Vengono definiti anche, si notava poco sopra, "captatori informatici" perché hanno la caratteristica di *captare* qualsiasi tipo di informazione sul computer o telefono preso di mira. Sono utilizzati dalle forze dell'ordine ma esistono programmi con funzionalità simili che sono venduti anche per un utilizzo in ambito aziendale.

e) controllo della posizione e dello spostamento del lavoratore utilizzando ricevitori satellitari e sistemi GPS. Si tratta di casi molto frequenti. Il GPS può essere collegato a una vettura (quindi indipendentemente da chi la guida) o a un dispositivo telefonico riferito a una persona o assegnato alla stessa. Il soggetto può essere messo in condizione di disattivare, o meno, questo sistema di controllo.

f) controllo effettuati dall'amministratore di sistema analizzando i file di log del server aziendale o dei singoli computer. L'amministratore di sistema è il soggetto che può vedere *tutto*, sia su richiesta del datore di lavoro, sia di sua iniziativa (ma sempre nell'ambito delle mansioni lavorative che lo riguardano, e non per pura curiosità o altri fini illeciti). Può fare a meno di codici e password e generare in ogni momento una radiografia di tutto ciò che accade sul sistema, pur nei limiti delle sue mansioni lavorative.

Ciascuno di questi tipi di controllo pone all'interprete problemi specifici. In tutti i casi, rimane il divieto del controllo occulto, anche se alcuni degli strumenti che si sono citati hanno, nell'essere travisati e occulti, la loro essenza tecnologica.

5. Controllo occulto, controllo indiscriminato e pervasività dei controlli.

Gli esempi elencati poco sopra coinvolgono strumenti che non distinguono, e non separano, attività lavorativa da attività personale, e che possono intercettare ogni azione (anche, ad esempio, eventuali e-mail personali presenti sul computer fornito dal datore di lavoro). Solitamente operano "a strascico", carpendo tutti i dati e lasciando al controllore il compito di separare le informazioni, e in maniera indiscriminata.

Il controllo occulto cambia anche prospettiva, nell'era tecnologica. L'idea era, prima, quella alla base di una telecamera nascosta o di un ascoltatore terzo agganciato alla linea telefonica. Oggi non è facile che il controllato abbia una *comprensione* piena del livello di controllo cui si può arrivare, anche perché lo stesso può essere *modulato* dal datore di lavoro. Comprendere il tipo di controllo richiede, a volte, competenze informatiche avanzate. Il principio di base è che tutto è controllabile, ogni singola operazione. Non è un caso che il Garante insista nelle *informative*, ossia nella necessità di specificare al lavoratore nel dettaglio i controlli come sono effettuati e quali dati si possano vedere. Gli strumenti più complessi e più costosi per il controllo a distanza sul posto di lavoro e sulla rete aziendale sono di solito composti da moduli e da regole. I moduli permettono di aggiungere o togliere strumenti di controllo (ad esempio: modulo per il telefono cellulare, modulo per la navigazione in rete, modulo per la posta elettronica, modulo per le chat, e così via) mentre le regole consentono di allargare o stringere la profondità di controllo, da un livello di controllo anonimo a uno specifico e mirato nei confronti di tutte le comunicazioni afferenti al soggetto.

Le seguenti sono alcune modalità di controllo comuni, con relativi bersagli, tipiche dei software per il controllo più utilizzati, oggi, in azienda:

1) controllo della posta elettronica, inteso, da un lato, come controllo di quante e-mail inviate e ricevute in un dato lasso di tempo e dei rispettivi destinatari e mittenti e, dall'altro, come il controllo che consente di apprendere il testo del messaggio e di consultare gli allegati, di verificare l'identità di chi ha spedito la mail o ha acceduto con le credenziali, di recuperare dal server e-mail cancellate, di duplicare la casella di posta elettronica (per cui le e-mail inviate e ricevute arrivano sia al soggetto che le riceve/manda sia a un terzo, ad esempio un amministratore di sistema o un datore di lavoro), di accedere alla casella del lavoratore e spedire e-mail in sua vece o leggere e-mail se lui è assente, di intercettare una e-mail prima che giunga al soggetto legittimo destinatario;

2) controllo della navigazione in Internet: siti web consultati, in quale orario e per quanto tempo, le pagine salvate, l'analisi della cronologia anche delle ultime settimane, la verifica dell'accesso a una casella di e-mail privata o a siti web di home banking;

3) controllo del disco del computer e dei suoi contenuti, come documenti personali, video, fotografie, cartelle personali, procedure d'installazione di software particolari, recupero di dati e informazioni cancellate;

4) inserimento di strumenti di accesso remoto che forniscono al datore di lavoro l'accesso pieno alle attività del computer altrui e gli permettono di seguire tutte le attività, esattamente come se ci fosse una telecamera puntata sul monitor del computer del dipendente, o da usare come microspia ambientale (registrazione delle conversazioni), telecamera (registrazione video ambientale attivabile da remoto) o sistema di pedinamento elettronico (attivazione del GPS);

5) controllo simile sugli apparecchi telefonici forniti: apprensione dei messaggi in entrata e in uscita, registrazione delle telefonate, chat e gruppi su WhatsApp, consultazione della cronologia dei siti web visitati.

Una conoscenza accurata dei metodi di controllo permette di attivare procedure per sfuggire a un simile controllo, anche utilizzando appositi software in tal senso.

Il controllo può essere occulto secondo tre accezioni:

1) occulto perché non altera visibilmente le funzionalità del sistema, per cui il lavoratore non se ne accorge;

2) occulto perché non è comprensibile dal soggetto controllato (ossia agisce su aspetti tecnici che il soggetto non può conoscere);

3) occulto oppure perché è effettuato su dispositivi che non sono nella disponibilità del soggetto, ad esempio i server aziendali o gli strumenti restituiti al datore di lavoro a fine giornata e successivamente analizzati.

6. Considerazioni conclusive: i problemi all'orizzonte.

In un sistema di controllo post-moderno quale quello disegnato poco sopra, i problemi che si pongono all'interprete sono numerosi.

Il primo è, a nostro avviso, quello della conoscenza in capo al lavoratore e dell'informativa da fornire per descrivere come sono effettuati tali tipi di controllo. Una volta era semplice illustrare il funzionamento di una telecamera. Gli unici parametri da spiegare erano il campo di ripresa, se i dati fossero solo in formato video o anche audio, e se (e per quanto tempo) le registrazioni fossero conservate. Oggi gli strumenti di controllo sono tecnicamente assai complessi e addirittura possono reagire, nelle modalità, ai comportamenti del lavoratore (per cui intervengono con una segnalazione quando, ad esempio, un soggetto sta per collegarsi a un determinato sito web o sta per installare un determinato software). Se non si comprende l'essenza del controllo, non se ne può comprendere a fondo il rischio. Vi è quindi la possibilità che oggi numerosi tipi di controllo risultino occulti non solo perché non visibili ma anche perché non comprensibili.

Un secondo punto è l'aspetto delicatissimo dei controlli indiscriminati. Tutti i sistemi più evoluti, oggi, agiscono sia sui dati correlati alla prestazione lavorativa sia su eventuali dati personali che stiano "contaminando" la scena del posto di lavoro ma, che, in alcuni casi, possono essere "normali" (si pensi al collegamento a determinati siti in un momento di pausa). L'unione, oggi, tra acquisizione dei dati informatici correlati alla prestazione lavorativa e altri dati che possono essere legati al lato personale del lavoratore comporta l'aspetto delicato della separazione di detti dati. La procedura di separazione dei dati è molto complessa e richiede grandi risorse. E molto spesso dispositivi quali un telefono cellulare, un tablet o un computer portatile arrivano a contenere, nel corso del tempo, anche dati personali del possessore.

Infine, particolarmente preoccupanti sono due tipi di software che permettono di spiare le attività all'insaputa del lavoratore (ad esempio perché inserite surrettiziamente nei dispositivi forniti dal datore di lavoro) e di attivare a distanza i dispositivi costringendo il lavoratore a consultare e-mail, comunicazioni o documenti anche al di fuori dell'orario di lavoro. Sono due sistemi di controllo da remoto che non hanno precedenti nella storia della tecnica, e che certamente pongono spunti di riflessione nuovi.

Bibliografia.

P. Costanzo, *Note preliminari sullo statuto giuridico della geolocalizzazione (a margine di recenti sviluppi giurisprudenziali e legislativi)*, *Diritto dell'Informazione e dell'Informatica*, 2014, 3, 331.