QUESTIONI DI INTERESSE PUBBLICO LEGATE ALL'ESTERNALIZZAZIONE DEI SERVIZI INFORMATICI DEL MINISTERO DELLA GIUSTIZIA: ATTIVITA' GIUDIZIARIA A RISCHIO DI INFILTRAZIONI?
PROGETTO DI PROPOSTA ALTERNATIVA IN FAVORE DELL'ANM.

di Lidia Undiemi[*]

La politica di esternalizzazione dei servizi informatici attuata dal ministero della Giustizia presenta rilevanti questioni di interesse pubblico.

L'aspetto che sicuramente desta maggiori preoccupazioni è l'affidamento ai privati dell'organizzazione informatica dell'attività giudiziaria.

Quello che si contesta, si badi bene, non è il ricorso all'informatizzazione dei processi organizzativi dei palazzi della Giustizia, che è ovviamente una necessità incontestabile, bensì il modo attraverso cui ciò è stato progettato.

Da una prima analisi della documentazione, pare che il ministero della Giustizia abbia praticamente ceduto a terzi la gestione delle informazioni relative all'attività giudiziaria. La domanda sorge spontanea: esiste un oggettivo pericolo che nel corso delle indagini il lavoro del magistrato finisca nelle mani di soggetti privati con tutte le conseguenze del caso? Di sicuro, non rassicura il fatto che l'assistenza informatica, almeno in parte, sarà gestita dalle società private attraverso dei call center con accesso da remoto, e forse potenzialmente in tutte le aree della postazione di lavoro del magistrato.

E' chiaro che un formale protocollo di sicurezza non è sufficiente per eliminare tale pericolo, dati i mezzi tecnici attraverso cui i privati potranno gestire il servizio.

Ma nell'ipotesi in cui un operatore di call center violasse i sistemi di sicurezza, su chi ricadrebbe la responsabilità? E' la risposta a questa domanda che consente di rendere meno incerti i confini dell'operazione.

Per cominciare, il principale effetto dell'esternalizzazione è una sorta deresponsabilizzazione della p.a. nei confronti dei cittadini. L'affidamento a fornitori esterni di determinati servizi pubblici implica infatti che il cittadino, nei casi di cattiva amministrazione dell'attività esternalizzata, possa solo rivalersi nei

[*] Membro della Lega Italiana dei Diritti dell'Uomo e dell'Associazione Nazionale dei Lavoratori Esternalizzati. Dottoranda di ricerca presso il Dipartimento di Diritto dell'Economia, dei Trasporti e dell'Ambiente.

confronti del privato. In altri termini, il rapporto pubblica amministrazione-cittadino si trasforma in un rapporto tra privati, con la conseguenza che la gestione della cosa pubblica segue prevalentemente, se non addirittura esclusivamente, mere logiche di mercato.

Quanto poi al personale addetto ai servizi ceduti, le conseguenze della privatizzazione sono nella maggior parte dei casi pessime. Essere un pubblico dipendete fornisce garanzie di stabilità del posto di lavoro e di rispetto dei diritti che una società <<commessa-dipendente>> non sarà mai essere in grado di fornire. Molti dei lavoratori dell'Assistenza Tecnica Unificata del ministero della Giustizia, che hanno fino ad oggi supportato l'assistenza informatica nei tribunali, sono stati licenziati e molti altri lo saranno a breve.

Questa, ovviamente, è un'ulteriore conseguenza negativa per il cittadino. Come può, in termini di sicurezza ma anche di professionalità, un lavoratore di una qualsiasi società privata offrire le stesse garanzie di un lavoratore stabile soggetto al diretto controllo della p.a.? La risposta è ovvia, tale privatizzazione comporterà probabilmente una consistente perdita di controllo sulle persone che metteranno le mani sulla gestione informatica dei dati giudiziari.

A nulla vale, poi, che nei contratti quadro si stabiliscano delle penali a carico della parte inadempiente. Primo, l'eventuale risarcimento andrebbe a favore della pubblica amministrazione e non del cittadino. Secondo, si tratta di un risarcimento di natura economica, riferito esclusivamente al livello di qualità del servizio, e non anche in specifica relazione alla gestione dei sistemi di sicurezza.

Anzi pare che il fornitore esterno si sia ben guardato da un'eventuale responsabilità in quest'ultimo senso. Tra le varie ipotesi di Forza maggiore previsti nell'art. 24 del Contratto Quadro relativo al lotto 1 (n. 4/2007)[1], si prevede infatti anche il sabotaggio, che è, e le parti ne sono ben consapevoli, uno dei metodi più conosciuti di infiltrazione informatica. Sulla base di tale accordo, si arriverebbe all'assurda conclusione che nell'ipotesi di deliberata azione volta all'intralcio e all'indebolimento dell'attività giudiziaria per il tramite dei servizi informatici le parti non hanno alcuna responsabilità. Ma poi, perché prevedere inoltre, fra i casi di forza maggiore, gli atti di Governo, delle autorità giudiziarie, delle autorità amministrative e/o delle autorità di regolamentazione indipendenti?

[1] Nessuna Parte sarà responsabile per qualsiasi perdita che potrà essere patita dall'altra Parte a causa di eventi di forza maggiore (che includono, a titolo esemplificativo, disastri naturali, terremoti, incendi, fulmini, guerre, sommosse, sabotaggi, atti del Governo, autorità giudiziarie, autorità amministrative e/o autorità di regolamentazione indipendenti) a tale Parte non imputabili (comma uno).

Anche volendo richiamare la tutela prevista nel d.lgs. n. 196/2003 in materia di trattamento dei dati personali, che è sicuramente una strada da intraprendere, si tratterebbe comunque del *diritto individuale* alla privacy e non del *diritto collettivo* alla giustizia.

Ovviamente, il rischio di infiltrazioni con accesso da remoto esiste anche nell'ipotesi di gestione interna dei servizi informatici, ma in misura estremamente ridotta grazie al diretto controllo del dipendente pubblico da parte dell'amministrazione. C'è da chiedersi allora, perché gestire i dati dell'attività giudiziaria direttamente su un database centralizzato su server da remoto? Esiste attualmente la necessità che i tribunali si scambino le informazioni? Ciascun singolo tribunale non ha una propria organizzazione interna autonoma? Per quanto riguarda la mera attività amministrativa, e dunque escludendo l'attività del singolo magistrato, la centralizzazione dell'organizzazione di lavoro riferita al singolo tribunale è sicuramente utile. Solo così, infatti, i vari uffici amministrativi possono comunicare in modo efficiente ed efficace in quanto possono scambiarsi i dati, opportunamente classificati, in tempo reale.

La verità allora è che bisogna distinguere due diversi ambiti: l'attività amministrativa dei tribunali e quella investigativa del magistrato. L'informatizzazione centralizzata della prima non dovrebbe comportare grossi problemi di sicurezza. Tuttavia, perché bisogna centralizzare a livello nazionale e non a livello di singolo tribunale? Diversamente, l'attività di indagine della magistratura non dovrebbe essere centralizzata nemmeno a livello di singolo tribunale. In questo senso, bisogna anzitutto comprendere in dettaglio se ed in che modo la gestione da remoto coinvolgerà il lavoro dei magistrati.

Altre preoccupazioni sorgono in merito al comportamento dei privati nel mercato delle esternalizzazioni. Spesso le società appaltatrici riescono a loro volta a deresponsabilizzarsi attraverso la creazione di una o più società, direttamente o indirettamente controllate, che, attraverso il ricorso al subappalto, fungono da contenitori di pezzi di attività. Ne consegue che, poiché rispetto alla società controllante essi rappresentano distinti centri di imputazione di rapporti giuridici, chi risponde dei danni eventualmente cagionati dalla società subappaltatrice? Se non per espressa previsione, chi cede in subappalto attività che gli sono state commissionate dall'operatore pubblico non deve rispondere con il proprio patrimonio per l'attività svolta dalla subappaltatrice, a meno che non si dimostri l'abuso di personalità giuridica.

Infine, si consideri che anche la disciplina relativa ai gruppi societari prevede specificatamente solo due tipi di responsabilità, della controllante nei confronti dei soci e dei creditori della controllata, e dunque nessuna disposizione in favore degli altri soggetti coinvolti a vario titolo nell'attività d'impresa, compresi i lavoratori.

Tirando le somme, nessuno risulta adeguatamente responsabile di una eventuale violazione dell'attività giudiziaria, forse, al limite, un disgraziato operatore di call center, magari assunto con un contratto a progetto di seicento euro al mese.

La Magistratura rischia di subire un serio attacco dall'interno, nella peggiore delle ipotesi devastante e dalle conseguenze incalcolabili per l'intera collettività.

L'unico modo per prevenire tale pericolo è quello di comprendere fino in fondo i reali termini della privatizzazione.

Per tale ragione, è necessario che la Magistratura attui un programma di lavoro volto al raggiungimento di tale obiettivo, soprattutto attraverso il coinvolgimento degli esperti informatici dell'Assistenza Tecnica Unificata, cui va il merito di avere sollevato la questione.

In questa direzione, occorrerebbe approfondire l'eventuale esistenza di incompatibilità tra tale politica di outsourcing ed alcune disposizioni di legge. Fra queste:

- la normativa in materia di protezione dei dati personali (d.lgs. n. 196/2003), specie in riferimento ai trattamenti in ambito giudiziario;
- il Codice dell'amministrazione digitale (d.lgs. n. 82/2005);
- il Testo unico sugli appalti pubblici (d.lgs. n. 163/2006).

Tutto questo dovrebbe essere finalizzato alla formulazione di una proposta alternativa di informatizzazione dell'attività giudiziaria, che non comporti il trasferimento dei dati e delle informazioni relative alle indagini condotte dai magistrati, ovviamente una volta verificato che quella attuale risulta impostata in tal senso.

In questa direzione, una forma di sana e proficua applicazione della tecnologia nel settore della Giustizia potrebbe essere la creazione di un sistema informatizzato di raccolta ed elaborazione delle sentenze, diretti alla individuazione dei contenziosi che generano maggiori conflitti sociali a livello nazionale. Il legislatore, a questo punto, sarebbe in grado di realizzare proposte normative molto vicine alle esigenze della collettività.

CONTRIBUTI IN FAVORE DEL PROGETTO DI PROPOSTA ALTERNATIVA

1. Esternalizzazioni e precarietà: l'Assistenza Tecnica Unificata nel settore della Giustizia[2]

di Lidia Undiemi

Tra le diverse forme di gestione ed amministrazione della giustizia esistono le politiche di esternalizzazione, che consistono nell'affidamento a terzi di processi organizzativi riguardanti l'attività giudiziaria.
L'outsourcing dei servizi informatici è un percorso che il ministero della Giustizia segue ormai da diversi anni[3].
Rispetto all'ampio ventaglio di questioni che possono emergere in relazione a tale scelta, lo scopo in questa sede è quello di descrivere brevemente la vicenda dei lavoratori "precari" utilizzati per lo svolgimento del servizio informatico e di affrontare, di riflesso, i rischi derivanti dalla fornitura esterna, che sono stati ben documentati in un recente articolo[4].

Da circa 15 anni, a fronte di esigenze di ammodernamento della struttura pubblica, il Ministero affida la gestione dell'assistenza informatica giudiziaria, la cosiddetta Assistenza Tecnica Unificata (ATU), a società private.
Tale operazione ha coinvolto centinaia di lavoratori, difficilmente quantificabili in quanto assunti da diverse società operanti nel territorio nazionale, e comunque attraverso svariati contratti di lavoro, talvolta addirittura stipulati presso più società, a seconda dell'affidamento della commessa ad un soggetto giuridico piuttosto che ad un'altro. Circa la metà di essi hanno perso il posto di lavoro.
Ciò non significa che non esistono esperti informatici presso gli organici dell'Amministrazione (strutture DGSIA/CISIA), ma solo che questi non sono sufficienti per lo svolgimento della maggior parte delle attività che sono appunto svolte all'esterno.

---

[2] Articolo pubblicato su diritto.it in data 18/06/2009.
[3] I dati e le informazioni contenuti nel presente scritto sono principalmente quelli elaborati dal comitato dei lavoratori ATU.
[4] V. Carlo Sarzana, L'assistenza Tecnica Unificata nel settore della Giustizia: informatici usa-e-getta?, in diritto.it. Si farà costante riferimento a questo articolo per la ricostruzione dell'esternalizzazione.

Definire l'oggetto dell'outsourcing dei servizi informatici è un compito estremamente difficile, sia per la natura del servizio in sé che per la frammentazione della gestione delle attività informatiche in favore di diverse aziende private esterne.

Il servizio informatico è composto infatti da svariate componenti: gestione di sistemi, elaborazione di specifici software, hosting, progettazione e realizzazione di siti web, accesso alle applicazioni in modalità web, gestione delle postazioni di lavoro e tante altre. Ed è proprio per tale ragione che è possibile affidare la realizzazione del servizio a più società.

Tuttavia, l'eccessiva frammentazione nella gestione delle attività informatiche comporta maggiori difficoltà in termini di azioni di controllo e di interventi correttivi, qualora si verificasse una incongrua gestione da parte dei fornitori esterni. E la situazione si complica in modo esponenziale se si tiene conto che spesso i servizi subiscono ulteriori suddivisioni a causa del ricorso al subappalto.

Sicuramente, uno degli aspetti più importanti di tale politica di outsourcing è il rischio di una notevole perdita di tutela nei confronti della magistratura, dei lavoratori e dei cittadini in generale, proprio in ragione della privatizzazione di parte dell'attività del sistema giudiziario.

Prima di entrare nel merito di tale questione, è necessario ripercorrere brevemente l'evoluzione della terziarizzazione del servizio informatico.

L'esternalizzazione del servizio informatico di Assistenza Tecnica Unificata presso tutti gli uffici giudiziari ha avuto inizio a partire dal 1989.

Dal 1997 e sino al 2007 il ministero della Giustizia ha affidato l'appalto dell'Assistenza Tecnica Unificata (chiamato così fino al 2008) a singole ditte sparse sul territorio nazionale.

Sulla base di quanto affermato in sede di interrogazione parlamentare[5], i lavoratori di tali società appaltatrici risultano impiegati nella gestione dei dati sensibili e dei server, nell'amministrazione delle reti, nella gestione e manutenzione del parco hardware e software, nel supporto totale degli utenti, nella formazione ed altro, con ciò rappresentando l'unico punto di riferimento per ogni problema di natura informatica di Tribunali e Procure, in rapporto diretto con

[5] Legislatura 16 Atto di Sindacato Ispettivo n° 3-00608 Atto n. 3-00608 Pubblicato il 11 marzo 2009 Seduta n. 169 Armato, De Luca, Incostante - Ai Ministri della Giustizia e del Lavoro, della Salute e delle Politiche sociali. Si consideri inoltre l'interpellanza presentata da Arturo Scotto il 3 maggio 2007 Seduta n. 151.

magistrati, cancellieri ed operatori.

Con bando pubblicato nella G.U. del 29/11/2004 è stata lanciata la gara avente ad oggetto la fornitura di servizi di Assistenza Tecnica Unificata, riferita a vari lotti corrispondenti a diverse aree geografiche.

Nel frattempo è entrata in vigore la legge finanziaria 2005 (l. n. 311/2004), che all'art. 1 dispone una serie di criteri finalizzati al miglioramento dell'efficienza operativa della pubblica amministrazione ed al contenimento della spesa pubblica (commi 192, 193 e 194).

E' stata prevista inoltre l'attuazione del DPCM del 30/05/2005, finalizzato alla individuazione delle applicazioni informatiche e dei servizi per i quali si rendono necessari razionalizzazioni ed eliminazioni di duplicazioni ecc (art. 1).

Sempre nello stesso anno è stato pubblicato il d.lgs. n. 42/2005 relativo Servizio Pubblico di Connettività (SPC) avente diverse funzioni, fra cui la fornitura di servizi di connettività condivisi dalle pubbliche amministrazioni interconnesse e l'interazione della pubblica amministrazione centrale e locale con tutti gli altri soggetti connessi ad internet (art. 6).

Ad aprile del 2005, intanto, le aziende Ois.Com/GruppoCM&C perdono l'appalto relativo alla gara nazionale che vede il suddetto consorzio al terzo posto, la Getronics al primo e la Ibm/Abaco/Sisge al secondo nei vari lotti. Comincia così un periodo nero per gli informatici che svolgono da anni il proprio lavoro presso le sedi giudiziarie, dato che la sorte dei loro contratti di lavoro è legata alla sopravvivenza nel mercato delle società che hanno perso la commessa. All'orizzonte si prospetta il licenziamento, non essendo nemmeno prevista nei contratti di appalto alcuna <<clausola di salvaguardia>> per il personale già operativo negli uffici giudiziari.

Segue l'aggiudicazione del bando emesso nel 2004 relativo all'Assistenza Tecnica Unificata (D.M. 5/12/2005) da parte del Raggruppamento Temporaneo di Imprese (Ibm, Sisge, ecc), impugnata dinanzi al TAR del Lazio che annulla la gara avendo riscontrato gravi irregolarità nelle procedure seguite dal Ministero[6].

A questo punto, l'Amministrazione, anziché rinnovare il bando di gara per l'affidamento del servizio informatico, decide di separare l'oggetto dell'assistenza aderendo all'SPC e provvedendo diversamente per gli applicativi civili e penali.

Intanto il CNIPA indice una gara a procedura ristretta (n. 1/2006, bando di gara pubblicato nella G.U.C.E. del 6/4/2006) per l'affidamento della progettazione,

[6] Il ministero ha proposto appello al Consiglio di Stato, ma ha poi rinunziato al ricorso stesso per cui il processo è stato cancellato dal ruolo all'udienza del 23/12/2007.

realizzazione e gestione dei servizi di siti web e conduzioni di sistemi (lotto 1) e dei servizi di interoperabilità evoluta e cooperazione e sicurezza applicativa (lotto 2) in favore della pubblica amministrazione nell'ambito SPC.
La gara relativa al lotto 1 (contratto-quadro 4/2007) è stata vinta dal RTI rappresentato da Telecom Italia Sp.a., Datamat S.p.a., Elsag S.p.a. ed Engineering Ingegneria Informatica S.p.a. Il lotto 2 (contratto-quadro 5/2007) è stato invece affidato al RTI rappresentanto da EDS Electronic Data Systems Italia S.p.A. (mandataria) e Almaviva The Italian Innovation Company S.p.A. (mandante).
Per quanto riguarda gli applicativi, giacché il contratto-quadro 4/2007 non contempla l'essenziale servizio di assistenza applicativa ai sistemi in uso, si è resa necessaria la stipulazione nel 2008 di un apposito contratto con RTI composto da CM Sistema S.p.a., Almaviva S.p.a., Eutelia S.p.a., Ois.Com., ISI Ingegneria dei Sistemi Informativi S.r.l., Sistemi Informativi S.p.a. a Società OIS.Com Consorzio. In questo modo si è riusciti ad assicurare l'erogazione dei servizi applicativi al sistema <<*legacy*>> in uso negli uffici giudiziari, in attesa del definitivo passaggio ai servizi <<*web based*>>.
Pare dunque che nonostante il Ministero abbia preso accordi con nuove società, per il momento l'assistenza informatica, precisamente applicativa, continua ad essere svolta dai lavoratori delle aziende che già in passato si sono occupati di tale servizio. Ma questa è ovviamente una fase transitoria, che cesserà di esistere quando sarà attuato il definitivo passaggio ai nuovi sistemi. Le nuove società, intanto, hanno predisposto dei call center.
Che fine faranno i lavoratori legati al vecchio sistema? Non si sa.

Prima di fare delle considerazioni sulla posizione dei lavoratori ATU nei confronti del Ministero e delle svariate società private che direttamente o indirettamente decidono le sorti del loro posto di lavoro, è necessario aprire una parentesi sul mercato dell'outsourcing.
In Italia un lavoratore coinvolto in politiche di esternalizzazioni è sostanzialmente un lavoratore precario. Non importa se è stato assunto con un contratto di lavoro subordinato o "a progetto", perché, in ogni caso, finita la commessa che consente all'azienda appaltatrice di pagare gli stipendi finiscono tutti in mezzo a una strada.
E non bisogna nemmeno illudersi se si è stati assunti con un contratto di lavoro <<stabile>> da una grande impresa con una elevata solidità patrimoniale: lo strumento del trasferimento di ramo di azienda *ex* art. 2112 c.c. consente all'impresa

di trasferire settori della propria attività ad altre imprese, compresi i lavoratori che, secondo quanto stabilito dal suddetto articolo, non possono opporsi al proprio trasferimento. E' così che sono nate moltissime aziende commessa-dipendenti.
Il meccanismo di base è in effetti semplice, e trae forza da vuoti normativi sparsi nel sistema giuridico e da una notevole disinformazione circa gli strumenti di tutela in favore dei lavoratori messi a disposizione dalla legge in queste specifiche circostanze.
Si pensi ad esempio all'ipotesi in cui l'imputazione di un ramo d'azienda ad una determinata società risulti finalizzata ad un intento fraudolento. Il fenomeno, largamente diffuso, si manifesta essenzialmente attraverso la costituzione di una pluralità di società di capitali, le cui azioni o quote appartengono ai medesimi soggetti, al solo scopo di eludere l'applicazione di norme imperative di legge. Lo schema di creazione delle società fittizie dipende dall'obiettivo che si intende raggiungere. Si può attuare la costituzione di più società, anziché di una sola con un numero rilevante di dipendenti, al solo fine di evitare il raggiungimento della soglia numerica prevista per l'applicabilità della normativa sui licenziamenti collettivi e della tutela reale sancita *ex* art. 18 della l. n. 300/1970. Oppure, con lo scopo di licenziare un certo numero di dipendenti senza passare per i costi e gli oneri previsti nell'ambito delle procedure di licenziamento collettivo, si decide di trasferire i lavoratori in una società destinata ad essere sciolta. O ancora si può creare artificiosamente una società in prossimità della cessione, controllata dall'effettivo cessionario, per evitare di vestire i panni del datore di lavoro nei confronti dei lavoratori appartenenti al ramo acquisito.
Quello che si censura in queste ipotesi è evidentemente l'abuso della personalità giuridica, ossia della <<alterità soggettiva che la creazione di una nuova società ha creato entro una entità soggettiva sostanzialmente unitaria>>.

Chiusa questa parentesi, si può adesso entrare nel merito della vicenda degli informatici dell'Assistenza Tecnica Unificata.
Occorre anzitutto specificare qual'è il tipo di rapporto che intercorre tra il Ministero e le società fornitrici del servizio informatico, gli informatici e le società fornitrici del servizio informatico, gli informatici ed il Ministero.
Il Ministero e le società fornitrici stipulano un accordo mediante la sottoscrizione di contratti di appalto. Per l'esecuzione dell'appalto la società deve assumere personale, e dunque stipula un contratto di lavoro con gli informatici che dovranno

occuparsi dell'assistenza tecnica presso gli uffici giudiziari. Ne consegue che fra il Ministero ed i lavoratori impiegati dall'appaltatore non intercorre alcun rapporto contrattuale: il Ministero usufruisce dell'assistenza informatica non come prestazione di lavoro, bensì come servizio da parte dell'appaltatore. Tuttavia, se si verifica che l'appalto ha come oggetto reale mere prestazioni di lavoro, la pubblica amministrazione incorre nell'interposizione illecita di manodopera ovvero nella somministrazione di lavoro al di fuori dei casi consentiti dalla legge[7].

Nel caso in cui il committente è un soggetto privato, la principale sanzione prevista in tale ipotesi è la costituzione diretta di un rapporto di lavoro in capo all'effettivo datore di lavoro. Sanzione altamente protettiva se si considera che l'interposizione è finalizzata alla deresponsabilizzare dell'effettivo utilizzatore.

Se invece si riscontra un appalto di mere prestazioni di lavoro nell'ambito della pubblica amministrazione, non è possibile ottenere la costituzione di un rapporto di lavoro subordinato tra essa ed il lavoratore. Ciò in quanto, anche se interviene l'elusione di cogenti norme legislative, si deve tenere conto nel settore pubblico della regola del pubblico concorso di cui all'art. 97 della Costituzione. Tale regola è poi concretamente salvaguardata con una serie di disposizioni legislative, che espressamente richiamano la nullità dell'assunzione effettuata senza l'osservanza delle prescritte procedure selettive. Ne consegue che la nullità dell'atto costitutivo del rapporto di pubblico impiego comporta unicamente la sussistenza di un rapporto di fatto con le conseguenze favorevoli di cui all'art. 2126 c.c. Secondo l'art. 36 del d.lgs. 165/2001, poi, nella fattispecie in questione il lavoratore interessato ha diritto al risarcimento del danno derivante dalla prestazione di lavoro in violazione di disposizioni imperative. Le due norme, sostanzialmente, stabiliscono una duplice tutela, ossia il diritto alla retribuzione ed il diritto al risarcimento del danno (aquiliano).

Detto ciò, è evidente che a prescindere dal tipo di tutela predisposta in favore del lavoratore, la pubblica amministrazione che ricorre all'appalto di mere prestazioni di lavoro viola disposizioni imperative. E la cessazione del comportamento illegittimo diventa un atto dovuto, con l'ulteriore impegno da parte dell'Amministrazione di interessarsi affinché i lavoratori coinvolti trovino un'adeguata collocazione.

---

[7] L'interposizione illecita di manodopera è stata per anni disciplinata dalla l. n. 1369/1960. Tale normativa è stata modificata in modo sostanziale dal d.lgs. 276/2003 che, abrogando la legislazione precedente, ha dettato una nuova regolamentazione attraverso cui ha ampliato le opportunità di ricorso legittimo alla somministrazione di lavoro (fornitura professionale di manodopera ai sensi dell'art. 2 e dell'art. 20), pur mantenendo un divieto generale di ricorso a tale fattispecie contrattuale al di fuori delle ipotesi previste dalla stessa legge, e comunque sottoponendo gli operatori ad uno specifico regime di autorizzazione amministrativa.

Da alcune testimonianze dei lavoratori ATU si evince chiaramente che essi stessi si definiscono <<di fatto lavoratori in intermediazione per il Ministero e quindi se ATU viene ridimensionata la società nel 99% dei casi scarica il lavoratore>>.
Ma queste sono ovviamente solo supposizioni, e quindi tale circostanza potrebbe essere confermata o smentita soltanto attraverso un eventuale ricorso in giudizio da parte dei lavoratori interessati. E qualunque sia la verità, la speranza è che tutto si risolva con il dialogo tra le parti.
Ma giusto per completare il quadro della situazione, c'è da dire che l'ipotesi di appalto di manodopera potrebbe effettivamente configurarsi qualora il servizio di assistenza informatica si riduca sostanzialmente nell'attività dei prestatori di lavoro presso gli uffici giudiziari, senza cioè che ci siano ulteriori mezzi (materiali ed immateriali) forniti dall'appaltatore. Al contrario, se l'attività comprende anche la realizzazione del software su cui si effettua l'assistenza allora si può quasi certamente parlare di appalto genuino.
Depone a sfavore di quest'ultima ipotesi l'analisi dei costi elaborata dal comitato lavoratori ATU per il contratto relativo all'anno 2006-2007. In particolare, pare che dai contratti di fornitura del servizio di assistenza sistemistica e applicativa unificata per alcuni distretti, il corrispettivo sia calcolato principalmente sulla base delle retribuzioni da corrispondere ai lavoratori. Dal prospetto si evince tra l'altro la convenienza economica della gestione delle risorse all'interno della pubblica amministrazione rispetto all'outsourcing.
E' necessario infine un accenno all'eventuale subappalto del servizio, nonché dei lavoratori. In questo caso, poiché sia il committente che l'appaltatore sono soggetti privati può applicarsi, nell'ipotesi di appalto di manodopera, la sanzione dell'assunzione diretta in capo all'effettivo utilizzatore. Solo dopo aver ottenuto questo è possibile agire in giudizio per chiedere all'Amministrazione il diritto alla retribuzione e il diritto al risarcimento del danno.
Gli informatici dell'Assistenza Tecnica Unificata meritano di essere stabilizzati e di continuare a svolgere il loro lavoro, anche sui nuovi applicativi.

La precarietà degli informatici dell'Assistenza Tecnica Unificata si ripercuote negativamente sull'intera collettività.
Frammentazione ed instabilità del posto di lavoro conducono alla dispersione di un patrimonio prezioso di professionalità.

E' altamente discutibile che i magistrati debbano chiamare uno sconosciuto ad un call center per avere assistenza, quando per anni hanno collaborato fianco a fianco con persone con cui hanno instaurato rapporti di fiducia. Non a caso, alcuni magistrati hanno richiesto un intervento urgente in favore di un lavoratore a causa del mancato rinnovo del suo contratto di lavoro con una delle società appaltatrici.
Come ha giustamente evidenziato un autore al quale si rimanda per approfondimenti[8], ai tecnici sono affidati anche i servizi di *backup* sia degli applicativi (quindi le banche dati di procure e tribunali) che della documentazione proveniente dagli utenti, magistrati compresi.
L'autore sottolinea inoltre il rischio del *system management* da remoto: alcuni uffici hanno decisamente rifiutato di fornire le richieste autorizzazioni allegando motivi di sicurezza (si veda ad esempio la nota del Tribunale di Salerno del 31/10/2008).

2. Brevi considerazioni su alcuni dei principali rischi derivanti dall'applicazione del Contratto Quadro n. 4/2007

di Giorgio Ciaccio[**]

Premesso che in campo scientifico l'analisi, la sintesi e la progettazione di un determinato bene e/o servizio si basano su criteri di ottimizzazione delle risorse/materiali e massimizzazione dei benefici. Nella specifica ipotesi della gestione dell'organizzazione dell'attività giudiziaria o di parte di essa, il raggiungimento di tali obiettivi deve essere necessariamente vincolato al rispetto di un fine superiore, ossia la garanzia concreta che i dati e le informazioni riferiti all'attività della magistratura non siano utilizzati per fini illegittimi.
Nell'ambito del Contratto Quadro n. 4/2007, riguardante l'affidamento di parte dei servizi informatici relativi al settore della giustizia, pare che il suddetto fine non trovi adeguato riscontro, con la conseguenza che il rapporto rischio-beneficio derivante dall'esternalizzazione delle attività informatiche si traduca, di fatto, in un pericolo per l'intera collettività.

[8] V. Carlo Sarzana, L'assistenza Tecnica Unificata nel settore della Giustizia: informatici usa-e-getta?, cit.
[**] Responsabile per Palermo della <<Casa della legalità e della Cultura>>. Laureando in Ingegneria delle Telecomunicazioni presso la Facoltà degli Studi di Ingegneria di Palermo.

A sostegno di ciò, si riportano di seguito alcune dei principali aspetti problematici riscontrati nel Contratto Quadro e nel relativo Capitolato Tecnico. Ci si riferisce in particolare agli artt. 3, 14, 17 e 21.

L'art. 3, che contiene la descrizione dell'oggetto del contratto[9], presenta diverse aree di rischio/minacce in ragione delle caratteristiche del servizio che può essere descritto in altri termini nel modo seguente:

- assistenza alla migrazione e presa in carico dei siti delle amministrazioni;
- messa a disposizione di infrastrutture logistiche, nell'ambito di un Centro Servizi rispondente ai requisiti di cui al successivo punto 4.1;
- messa a disposizione delle amministrazioni degli strumenti per gestire i contenuti del sito (content management);
- messa a disposizione presso il Centro Servizi, di cui al successivo punto 4.1, delle piattaforme hardware, software, e di rete necessarie per ospitare i siti delle amministrazioni; conduzione tecnica ed operativa delle piattaforme di cui al punto precedente;
- rendicontazione sull'utilizzo del servizio e sui livelli di servizio conseguiti.

La migrazione e la presa in carico dei siti implica un trasferimento di informazioni dalla P.A verso terzi. Anche se dall'accordo non si evincono con chiarezza le implicazioni del trasferimento, di sicuro si dovranno trasferire dei database contenenti, oltre alle informazioni di pubblico dominio ed accesso, anche le informazioni sui dati sensibili dei singoli utenti, interni ed esterni alla P.A., che hanno effettuato la registrazione on-line.

Fin da questo primo punto si evince il problema del trattamento dei dati personali, in quanto, affidando la gestione a soggetti privati esterni, non si ha la certezza di come saranno trattati tali dati, e soprattutto chi potrà visualizzarli.

In termini di responsabilità, assume rilievo la disposizione secondo cui nell'ambito dell'attività relativa ai servizi <<l'Aggiudicatario assume la responsabilità completa della gestione delle diverse componenti tecnologiche dell'Amministrazione curandone il buon funzionamento, la gestione proattiva, il monitoraggio e l'aggiornamento>> (comma b), esplicitamente descritto nel Capitolato Tecnico). Tale affermazione alimenta l'idea dell'inadeguatezza dell'esternalizzazione in

[9] Art.3: a) servizi di gestione di siti web suddivisi in: a.1) hosting di siti web; a.2) progettazione e realizzazione di siti web; a.3) supporto tecnico alle attività di tipo redazionale e gestione dei contenuti di un sito web; a.4) accesso ad applicazioni in modalità web; b) servizi di conduzione sistemi: b.1) gestione dei posti di lavoro; b.2) WAN e LAN Management; b.3) system Management; b.4) servizio integrato di PDL, WAN – LAN e System Management; b.5) asset Management; b.6) monitoraggio delle prestazioni di applicazioni.

commento, dato l'ampio potere di gestione riconosciuto alle società appaltatrici.
Ma l'argomento che desta maggiori preoccupazioni è sicuramente quello relativo al controllo da remoto delle postazioni di lavoro (PDL), le cui modalità di gestione, contenute nel comma b.1) sono espressamente descritte nel Capitolato Tecnico (punto 2.1.1)[10].
Di seguito l'analisi dei principali punti riconducibili a minacce/rischi.

1. controllo remoto dei PDL.

Cerchiamo di capire cos'è il controllo remoto. Il controllo remoto è la capacità di poter accedere e amministrare un computer distante anche migliaia di Km, standosene a casa davanti al proprio PC o in qualsiasi altra parte del mondo. L'accesso da remoto può avvenire grazie a particolari software che semplificano la collaborazione con persone ubicate in luoghi diversi. Il programma deve essere installato sia nel PDL della persona che chiede assistenza, sia sul computer di chi opera l'intervento. Per poter intervenire sul PDL, il <<tecnico-assistente>> (che si trova chissà dove e dall'identità sconosciuta) può accedere in totale autonomia e in background (in modalità non visibile all'utente), in tutte le aree (hard disk, periferiche, cartelle ecc.) del PDL.
Tale tecnica, che trova attuazione in determinati settori economici, non può trovare riscontro ed applicabilità nell'ambito della giustizia.
I rischi/minacce che si presentano sono tali da sconsigliare assolutamente tale tecnica di assistenza.
Per capire meglio quello che si potrebbe prospettare occorre fare un esempio. Si finga che un Magistrato, nel corso di un indagine, stia stilando un verbale con un

[10] Il servizio consiste nelle seguenti attività: 1. controllo remoto dei PDL; 2. mantenimento in efficienza dei PDL attraverso un costante monitoraggio del funzionamento di tutte le componenti (hardware, software di base, di produttività ed applicativo); 3. aggiornamento su richiesta dell'Amministrazione delle componenti software dei PDL (di base, di produttività ed applicative); 4. attivazione preventiva e su richiesta della manutenzione delle componenti hardware (incluse le stampanti, gli scanner ed altre periferiche), ricorrendo a fornitori terzi contrattualizzati dall'Amministrazione; 5. esecuzione di attività di ripristino del buon funzionamento dei PDL a seguito di anomalie su uno o più delle sue componenti software (di base, di produttività ed applicative); 6 .installazione/disinstallazione, su richiesta dell'Amministrazione, di nuovi PDL, resi disponibili dall'Amministrazione stessa; 7. adeguamento dei PDL in funzione della mobilità degli utenti nell'ambito lavorativo al fine di garantirne l'operatività a seguito di trasferimenti degli utenti stessi di sede, di stanza, cambiamento di ruolo e/o mansioni; 8. popolazione ed aggiornamento della documentazione (configurazione e tipologia) dei PDL per ogni sede dell'Amministrazione (registri di configurazione); 9. salvataggio e ripristino degli archivi residenti sui PDL in caso di intervento di manutenzione; 10. installazione e gestione di prodotti antivirus forniti dall'Amministrazione; 11. help desk per il supporto tecnico agli utenti dei PDL ed all'Amministrazioni; 12. assistenza on-site a richiesta all'Amministrazione; 13. analisi della qualità del servizio reso anche attraverso rilevazione della soddisfazione utente.

qualsiasi programma di scrittura. Ad un certo punto ha la necessità di stampare tale verbale, ma dopo diversi tentativi, non riesce e chiama il Centro Servizi per l'assistenza da remoto. L'operatore (che per il Magistrato sarà soltanto una mera voce non bene identificata) accederà al computer del Magistrato per verificare il tipo di errore segnalato. Ciò significa che l'operatore potrebbe entrare nelle cartelle del Magistrato, prendere visione del contenuto del computer e nella peggior delle ipotesi copiarsi qualche file, sistemare la problematica segnalata e chiudere l'assistenza.

Da questo semplice esempio si evince che per quanto di possa vantare l'intenzione di predisporre un sistema di sicurezza, non c'è nessuna certezza sull'operato del <<tecnico-assistente>>.
Nel caso più malizioso di utilizzo fraudolento dei dati, sarebbe sicuramente il Magistrato a pagarne *in primis* le conseguenze, in quanto dovrà cercare di dimostrare la sua estraneità ai fatti. Ma si ritroverebbe a dare la caccia ad i fantasmi, data l'eccessiva indeterminatezza dell'organizzazione esterna, specie se si considera che è possibile ricorrere al subappalto, così come previsto dall'art 21.1 del Contratto Quadro[11].
E' evidente che soltanto l'assistenza effettuata dal personale interno all'amministrazione è in grado di garantire un adeguato livello di sicurezza nell'ambito dell'organizzazione dell'attività giudiziaria.

2. mantenimento in efficienza dei PDL attraverso un costante monitoraggio del funzionamento di tutte le componenti (hardware, software di base, di produttività ed applicativo). 4. attivazione preventiva e su richiesta della manutenzione delle componenti hardware (incluse le stampanti, gli scanner ed altre periferiche), ricorrendo a fornitori terzi contrattualizzati dall'Amministrazione.

Questi due punti portano alla luce un altro problema legato direttamente alla sicurezza del palazzo di giustizia.
Per effettuare una manutenzione dei componenti hardware è necessario che il tec-

[11] Il Fornitore avrà facoltà, nel rispetto dei termini del presente articolo di fare affidamento sulle capacità di altri soggetti, nei limiti e secondo le condizioni di cui alla Lettera di Invito, a prescindere dalla natura giuridica dei suoi legami con questi ultimi. In particolare, sulla base di quanto dichiarato in sede di gara ed alle condizioni previste dalla legge, potranno essere affidati in subappalto i seguenti servizi: WAN e LAN Management; System Management; Asset Management; Realizzazione siti web; Redazione, gestione e contenuti web; Accesso ad applicazioni in modalità web; Gestione posti di lavoro; Monitoraggio.

nico si rechi *in loco.* Ma chi è questo tecnico? Se per caso un PDL non si avvia, il tecnico, se non è in grado di effettuare tutte le verifiche *in loco*, probabilmente porterebbe fuori dal tribunale il PDL per eseguire la riparazione. Per esempio, nell'ipotesi in cui il tecnico sia un delinquente ingaggiato da un mafioso che ha interesse ad ostacolare il Magistrato che indaga su di lui, l'attività giudiziaria potrebbe essere seriamente compromessa.

6. installazione/disinstallazione, su richiesta dell'Amministrazione, di nuovi PDL, resi disponibili dall'Amministrazione stessa

Se l'Amministrazione richiede la disinstallazione di un PDL, visto che il bene è di proprietà dell'Amministrazione, e la disinstallazione viene effettutata dalla ditta appaltatrice, che fine farà il computer ed in dati in esso contenuti?

9. Salvataggio e ripristino degli archivi residenti sui PDL in caso di intervento di manutenzione

Pericolosissimo. Nel caso di salvataggio e di ripristino dei dati, il tecnico dovrà effettuare una copia di backup della PDL, tale copia rimarrà in suo possesso. Vi sembra una cosa sicura considerando che il tecnico è un soggetto non chiaramente identificabile, magari assunto con un contratto <<precario>> da chissà quale società subappaltatrice?

11. help desk per il supporto tecnico agli utenti dei PDL ed alle Amministrazioni

L'help-desk sa benissimo chi è il suo interlocutore, ha la possibilità di visionare la postazione del PDL, mentre chi chiama non sa chi è il suo interlocutore.

12. assistenza on-site a richiesta all'Amministrazione

Stessa problematica dei punti 2 e 4.

Anche il comma b.2), riguardante <<Wan e Lan Management >> è esplicitamente descritto nel Capitolato Tecnico. E' necessario comprendere anzitutto qual è il significato dei termini Wan e Lan:

- LAN - *Local Area Network (rete locale)*, è uno strumento che consente di colle-

gare nodi relativamente vicini, tipicamente nell'ambito di uno stesso edificio.
- WAN - *Wide Area Network (rete geografica)*, collega invece nodi a qualunque distanza, anche planetaria.
Per semplificare il discorso possiamo considerare una Lan come diversi PDL collegati tra loro all'interno dello stesso tribunale, mentre una Wan può consistere nel collegamento dei PDL di un tribunale ai PDL di altri tribunali d'Italia.
La sicurezza delle reti è una problematica che nasce nel momento in cui si hanno più computer interconnessi fra loro: essi, infatti, offrono diverse vulnerabilità sfruttabili, più o meno facilmente, da terzi per intromettersi nel sistema ed intercettarne i dati. Ad oggi le metodologie di attacco alla rete sono divenute molto sofisticate, e ciò rende la sicurezza delle reti una tematica in continua espansione.
Possiamo sicuramente distinguere, o meglio valutare, la robustezza e la relativa sicurezza in base ai tipi di collegamento utilizzato.
La rete wireless presenta, rispetto ad una rete fissa, una maggiore potenziale vulnerabilità, per le sue caratteristiche intrinseche di apertura. Questa apertura nell'etere, che non presenta delle marcature perimetrali, potrebbe portare ad attacchi anche dall'esterno dell'edificio che ospita le postazioni di lavoro. Per questo sono stati definiti una serie di meccanismi di protezione che hanno lo scopo di rendere la sicurezza di una rete wireless quanto più vicina a quella di una rete fissa. La rete wireless nonostante sia più vulnerabile ha comunque dei vantaggi d'installazione molto più ridotti della classica interconnessione via cavo, ciò comporta in edifici di tipo storico una scelta quasi obbligata, soprattutto se si considera un espansione dei PDL o degli asset, ma certamente non sicura. La vulnerabilità non può però mai essere ridotta a zero, perché le stesse contromisure presentano, a loro volta, delle debolezze.
In riferimento al comma b.3), il Capitolato Tecnico contiene specifiche indicazioni sul <<System Management>>, in particolare: il servizio di System management si applica solo ai server presenti sulle reti LAN ed operanti con i seguenti sistemi operativi: Windows; Linux; Unix in tutte le sue versioni. Il servizio può essere erogato in modalità remota, ovvero con presidio on-site in relazione alle dimensioni dei server ed alle esigenze dell'Amministrazione (punto 2.3).

Per ciò che concerne la descrizione del servizio[12], si può supporre, poiché non si fa

[12] Descrizione del Servizio (punto 2.3.1) - Il servizio, in relazione alle modalità di erogazione di cui al successivo punto 2.3.2, può consistere in tutto od in parte nelle seguenti attività: 1. Conduzione operativa articolata in: 1.1 conduzione operativa dei server; 1.2 gestione dei salvataggi e

chiarezza, che il database contenente tutti i dati della P.A. rimanga di proprietà dell'operatore pubblico. Cosa si può dire, invece, della gestione dei salvataggi e degli eventuali ripristini di tutte le componenti (configurazioni hardware e software, file di configurazione, basi dati, …) prevista al punto 1.2? Per non parlare degli aspetti di cui ai punti 1.4 e 1.5 relativi alla gestione dei supporti di memorizzazione dei dati e delle stampe.

Anche l'<<Asset Management>> (comma b.5) viene richiamato nel Capitolato Tecnico[13].

Un *asset* è un'entità posseduta dall'azienda, di cui interessa tracciare il ciclo di vita. Partendo dalle realtà più semplici nelle quali gli *asset* di interesse sono i PC (desktop e portatili), si può arrivare a situazioni più complesse che prevedono la gestione dei software installati, degli apparati di rete, dei palmari, e qualche volta anche di apparati come gli ups, o i televisori LCD sui muri. Il servizio deputato alla gestione di queste entità viene chiamato, appunto, *Asset Management*.

Nel caso in esame tale gestione è totalmente demandata a soggetti terzi, con tutti i rischi più volte descritti della fornitura esterna.

Art. 14 - Locali messi a disposizione dall'Amministrazione

Nel Capitolato tecnico si evince chiaramente che il fornitore esterno avrà inoltre accesso ai locali dell'Amministrazione[14].

---

degli eventuali ripristini di tutte le componenti (configurazioni hardware e software, file di configurazione, basi dati, …); 1.3 gestione della distribuzione del software sui server sulla base della fornitura da parte dell'Amministrazione all'Aggiudicatario delle componenti software da distribuire; 1.4 gestione dei supporti di memorizzazione (DAT, CD, streaming tape, ...); 1.5 gestione delle stampe; 1.6 realizzazione / aggiornamento delle procedure di lavoro; 1.7 preparazione dei flussi di lavoro; 1.8 schedulazione e controllo dei lavori in produzione (sia quelli con frequenza predefinita che quelli a richiesta); 1.9 attivazione di terze parti per la manutenzione sulle componenti hardware (preventiva o su richiesta); 1.10 popolazione ed aggiornamento della documentazione (configurazione e tipologia) dei server per ogni sede dell'Amministrazione (Registri di configurazione).

[13] Descrizione del servizio (punto 2.5.1) - [...] Esso ha la finalità di tenere un inventario storico completo ed esaustivo dell'infrastruttura informatica ed amministrativa dell'Amministrazione presente nei Registri di configurazione. Il servizio è esclusivamente orientato alla gestione dei seguenti asset: componenti hardware (server e PDL), apparati attivi di rete, software di base, di produttività ed applicativo di mercato.

Il servizio consiste nelle attività di integrazione delle informazioni contenute nei Registri di configurazione di cui ai precedenti punti 2.1, 2.2 e 2.3 mediante acquisizione dalla documentazione amministrativa fornita in copia dall'Amministrazione delle informazioni rilevanti relative agli asset in esercizio (costi sostenuti per l'acquisto/canoni di locazione; data di acquisto od ingresso in esercizio dei nuovi asset; eventuali scadenze contrattuali) ed alla loro gestione nel tempo attraverso la popolazione ed aggiornamento dell'inventario degli asset.

[14] L'Amministrazione provvede ad indicare ed a mettere a disposizione del Fornitore, gratuitamente e non in via esclusiva, locali idonei all'installazione degli eventuali apparati del Fornitore

Ora, considerando che la P.A. ha il personale tecnico interno a sua disposizione, possiede i PDL e soprattutto i locali, perché sta esternalizzando dei servizi che potrebbe tranquillamente svolgere al proprio interno con un minimo di investimento aggiuntivo, rispetto all'enorme costo (in termini di sicurezza e di valore monetario dell'operazione) della gestione esterna? Chi entrerà nei palazzi di Giustizia?

Art. 17 – Corrispettivi dei servizi

Assolutamente complesso è il sistema di pagamento predisposto dalle parti[15].
Si prevedono una serie di corrispettivi a canone variabile, che dipendono dalla quantità di dati trattati. Nel mercato attuale queste variabili sono inversamente proporzionali al costo stesso del servizio su scala temporale. Uno degli esempi lampanti del mercato attuale è il costo del mantenimento di un server che è dimensionato alla mole dei dati che si devono trattare. Cinque anni fa il costo di tale server era basato sulla quantità di dati e quindi il corrispettivo era effettivamente legato ad un canone variabile, o meglio si stabilivano dei livelli prestabiliti in base alla quantità di dati che presumibilmente si sarebbero trattati. Ad oggi questa modalità è quasi sparita, grazie all'avanzamento tecnologico che ha consentito la diffusione dei canoni fissi forfettari.

3. I rischi derivanti dalla gestione e manutenzione da remoto delle postazioni di lavoro e dei server.

Contributo degli informatici ATU

Con la nota prot. N. 890 del 9 giugno 2009, relativa al "Dispiegamento di strumenti per la gestione e la manutenzione remota delle postazioni di lavoro e dei server", il Ministero (DGSIA Direzione Generale per i Sistemi Informativi Automatizzati) ha espresso l'intenzione di affidare ad operatori di call center la manutenzione dei computer degli Uffici Giudiziari italiani e l'assistenza agli

necessari all'erogazione dei servizi richiesti, con le modalità indicate nel Contratto esecutivo di fornitura (punto 14.1).

[15] I servizi di cui all'art. 3.1 lett. a) e b) ai fini delle modalità di calcolo dei corrispettivi sono suddivisi in: (i) servizi a canone fisso nell'arco dell'anno solare, in cui rientrano i servizi di cui ai punti a.1), a.3), b.1), b.2, b.3), b.4) e b.5) dell'art. 3.1; (ii) servizi a canone variabile nell'arco dell'anno solare, in cui rientra il servizio di cui al punto b.6) dell'art. 3.1; (iii) fornitura di prodotti con manutenzione MAC ed eventuale manutenzione MEV, in cui rientrano i servizi di cui ai punti a.2) e a.4) dell'art. 3.1 (punto 17.1).

utenti.

Per questo motivo intende far installare in ogni computer un programma che consentirà a questi operatori di vedere tutto quello che passa sullo schermo e di interagire con esso. Si assicura che il sistema sarà trasparente perché l'utente potrà vedere quello che succede e controllerà che l'operatore del call center faccia solo ciò che gli è stato chiesto. Questo è vero: anche se l'operatore lavorasse con molta velocità, gli sarebbe difficile rubare o modificare dati mentre l'utente sta guardando.

Il vero pericolo infatti è un altro, e finora nessuno ne ha parlato. Si intende fornire agli stessi operatori dei call center le abilitazioni di Amministratore di sistema e quindi il controllo remoto di tutta l'infrastruttura di rete, compresi i server.

I server dei Palazzi di Giustizia (computer più sicuri e <<capienti>>, accesi 24 ore su 24) sono posizionati in sale apposite ad accesso controllato e custodiscono tutti i dati, molti dei quali sono riservati (registri civili e penali, documenti dei magistrati e del personale amministrativo, ma anche i nomi e le password di tutti gli utenti ed i livelli di accesso di ciascuno).

L'accesso a queste informazioni avviene solitamente tramite i computer del palazzo ed è regolamentato da una complessa serie di permessi dati ad ogni singolo utente. Ogni utente avrà quindi accesso solo a determinate informazioni, come disposto dai capi degli uffici. Con una eccezione: gli Amministratori del sistema.

Gli Amministratori, in una rete informatica, sono utenti particolari a cui è permesso visionare ed intervenire su tutte le informazioni contenute nei server e nei computer degli utenti, proprio perché devono gestire questi permessi e la normale manutenzione.

L'Amministratore può svolgere le sue mansioni solo da un computer collegato alla rete interna del palazzo; non è solitamente permesso, per ovvi motivi di sicurezza, il collegamento dall'esterno sfruttando la rete della Pubblica Amministrazione o internet.

Nell'ambito della Giustizia questi <<super-utenti>> coincidono con i tecnici ATU, persone presenti fisicamente nei palazzi di Giustizia, che si interfacciano quotidianamente con utenti e dirigenti per tutte le questioni di assistenza ed organizzazione delle attività informatiche.

Si tratta di personale fornito da ditte esterne che hanno vinto l'appalto (o sono in regime di subappalto). Nel corso degli anni, le ditte a volte sono cambiate alla

scadenza dei contratti o per altre cause, ma finora il personale è stato quasi sempre lo stesso, in quanto spesso veniva riassorbito dalla nuova ditta vincitrice, assicurando una continuità di gestione e personale esperto.
Questi tecnici sono in genere presenti da molti anni (a seconda della sede, fino a venti), hanno letteralmente <<costruito>> le reti e le procedure informatiche dei Palazzi di Giustizia e si sono guadagnate la fiducia del personale in anni di collaborazione con gli Uffici. Ovviamente sono le persone più indicate a svolgere la manutenzione.
Negli ultimi anni, in questo rapporto di fiducia diretto tra magistrati e tecnici amministratori si è intromessa una serie di ostacoli, primo tra tutti la riduzione progressiva del numero dei tecnici per mancanza di fondi, in seguito l'introduzione dei call center.
Quasi tutti gli Uffici Giudiziari (sicuramente tutte le Procure e le sedi centrali dei Tribunali) sono attualmente dei cosiddetti <<presìdi fissi>>, sono cioè costantemente presidiati da uno o più tecnici fisicamente presenti in sede.
Sembra assurdo o quantomeno poco pratico che gli utenti per ottenere assistenza informatica debbano: telefonare ad una serie di call center (che rispondono da Genova o Cosenza a seconda della materia), parlare con degli estranei, fornire tutte le proprie generalità e spiegare, a fatica, il problema.
Tutto questo per ottenere, con molto ritardo, l'intervento dei soliti tecnici conosciuti, che spesso si trovano a pochi metri di distanza e magari sono già a conoscenza del problema e della relativa soluzione. Ad esempio perché si tratta di un problema tecnico ricorrente o perché già segnalato da un altro utente qualche minuto prima. Lo spreco di tempo e risorse è evidente.
Succede ad esempio che il call center si rifiuti di aprire la chiamata per un guasto, semplicemente perché risulta che il computer in questione non sia più coperto dalla garanzia del produttore. Da anni il Ministero non appalta più l'assistenza per i guasti fuori garanzia, perciò il computer guasto viene semplicemente accantonato, e se non ce n'è un altro disponibile l'utente resta senza fino alla prossima fornitura.
Tutti i tecnici in sede invece possono fare alcuni tentativi per far <<ripartire>> la macchina, oppure potrebbero procedere con la sostituzione del componente difettoso se il pezzo di ricambio è fornito dall'ufficio stesso.

Ora, con la gestione remota, si vogliono dare i permessi di Amministratore agli

operatori dei call center, i quali avranno la possibilità di intervenire dall'esterno degli uffici esattamente come i tecnici in sede, tranne che per gli interventi fisici sulle macchine. Questi ultimi, in assenza di personale in sede, subiranno un grave rallentamento in attesa che sia inviato un tecnico esterno.

Tutto questo viene fatto nell'ottica del risparmio di personale ed assicurando che tutti gli interventi saranno registrati su appositi registri informatizzati, sia negli Uffici controllati, sia presso il call center. Purtroppo non sono ancora stati diffusi i particolari sui registri e le altre misure di sicurezza che il Ministero attiverebbe presso il call center. Nemmeno al recente convegno di Torino sono state fornite indicazioni in tal senso.

Ma questa tracciabilità degli interventi comunque è un semplice controllo a posteriori che non garantisce riservatezza dei dati. Va sottolineato inoltre che come Amministratori gli operatori del call center avranno la possibilità di cancellare o modificare i registri informatizzati presso gli uffici, proprio perché i loro permessi di accesso sono totali.

Gli <<amministratori esterni>>, inoltre, potrebbero addirittura visionare o copiare l'intero contenuto dei server senza farsi notare, accedendo semplicemente ai dati come su una chiavetta USB, senza interfacciarsi con lo schermo (monitorato) degli utenti.

Finora i tecnici potevano effettuare queste operazioni solo nell'ufficio in cui erano presenti (e conosciuti), ma se verranno date le autorizzazioni al controllo remoto, gli operatori dei call center potranno effettuarle simultaneamente in tutti gli Uffici Giudiziari italiani, con conseguenti enormi pericoli per la sicurezza, per l'autonomia della Magistratura e per il segreto istruttorio.

Gli operatori del call center potranno semplicemente cercare un certo nominativo, contenuto nei documenti di un qualunque ufficio, e trovare tutte le informazioni relative ad un'indagine in corso.

Accedendo ai registri dei computer degli utenti, potranno sapere quando un magistrato è presente in sede, i suoi orari e le sue abitudini, <<leggendo>> quando accende e spegne il computer.

Inoltre accederanno al Re.Ge. e potranno consultare o modificare il registro degli indagati, il registro intercettazioni e qualsiasi altro dato presente.

Potranno installare qualsiasi programma nei computer all'insaputa dell'utente, compresi quei software (ad es. LogMeIn o TEAMVIEWER) che permettono di controllare i computer, e non solo dalla postazione al call center collegata alla rete

della Giustizia, ma anche da qualunque computer in internet, sfruttando la connessione tra la rete della Pubblica Amministrazione e internet.

Se poi cedessero ad altri questo controllo, si aprirebbero scenari inquietanti.

Una volta aperte le <<porte informatiche>> dei Palazzi di Giustizia (cioè i firewall, apparecchi che impediscono l'accesso dall'esterno) per lasciare entrare gli operatori del call center, sarà chiaramente molto più complesso gestire la sicurezza degli accessi, ed eventuali intrusioni potrebbero non essere mai scoperte o comunque rilevate con molto ritardo.

Inoltre gli operatori del call center non hanno nessuna informazione sugli utenti, cioè non sanno se chi li chiama sia un commesso o il Presidente del Tribunale o un Procuratore o addirittura un giornalista o un malintenzionato a conoscenza del numero da chiamare e che si spaccia per qualcun altro).

Ignorano anche la peculiare organizzazione delle risorse informatiche della singola sede e le sue procedure interne, in quanto in tutte le sedi esistono programmi creati dal personale interno.

Quindi il call center, anche in perfetta buona fede, potrebbe dare informazioni errate all'utente o fornire informazioni riservate ad un utente non abilitato a riceverle.

La grande maggioranza del personale amministrativo non ha le conoscenze di base idonee ad affrontare con la necessaria rapidità l'innovazione informatica, per questo il supporto dei tecnici presenti in sede è fondamentale per qualunque problematica relativa all'informatica.

Al di là delle loro mansioni contrattuali i tecnici ATU vengono infatti interpellati per consulenze informatiche di vario tipo.

Ad esempio accade spesso che il contenuto delle circolari relative all'informatica deve essere <<tradotto>> dai tecnici, perché il personale non ha le conoscenze necessarie a comprendere il linguaggio utilizzato.

In molte sedi i tecnici hanno poi sviluppato, nel corso degli anni, programmi informatici per la gestione di molti servizi che a livello nazionale ancora non esistono, ad esempio per la gestione del registro intercettazioni, dell'invio telematico delle notizie di reato a carico di ignoti da <<importare>> a Re.Ge., dei calendari delle udienze penali, del registro dei Corpi di Reato.

Solo i programmatori originali potranno prestare assistenza a questi applicativi, perciò la loro sostituzione con personale che non ne conosce nemmeno l'esistenza e che per giunta opera senza la presenza fisica in sede, porterà sicuramente al

blocco dei sistemi e gli uffici giudiziari saranno costretti a ritornare ai registri cartacei in attesa che arrivino i software nazionali.

Un esempio dei disservizi che possono accadere in assenza di questi tecnici ci viene dal Tribunale di Napoli, dove il mancato rinnovo del contratto ad un tecnico con sette anni d'anzianità (per cause ancora sconosciute agli Uffici Giudiziari) ha comportato il blocco dell'ufficio pagamenti del Tribunale dal momento che in assenza del tecnico più esperto, nessuno era in grado di fornire assistenza al sistema.

A nulla sono servite le lettere di protesta di ben 70 Magistrati del Tribunale e le successive interrogazioni parlamentari sull'argomento. Il posto è tuttora assegnato addirittura ad un <<primo impiego>>.