BUSINESS GUIDE TOLA COMPLIANCE

Pianificare la gestione dei dati elettronici & ed evitare responsabilità legali

di Cynthia L. Jackson

BAKER & McKENZIE

Cynthia L. Jackson

Partner, Baker & McKenzie LLP

Cynthia L. Jackson è uno dei partner dell'ufficio di Palo Alto, California di Baker & McKenzie, lo studio legale più grande del mondo con uffici in 38 Paesi. Cynthia Jackson è l'autrice di "Business Guide to Compliance", una pubblicazione concepita per formare i manager su questioni di conformità normativa e di conformità con i mandati e le ingiunzioni di tribunali e enti governativi e con i requisiti di e-discovery. Cynthia L. Jackson desidera esprimere il suo apprezzamento nei confronti di John Raudabaugh, partner dell'ufficio di Chicago, per il suo contributo alle sezioni sul monitoraggio dei dipendenti, tratto dal suo memoriale amicus curiae in *The Guard Publishing Company and Eugene Newspaper Guild,* presentato all'NLRB il 9 febbraio, 2007.

Cynthia Jackson rappresenta aziende in contenziosi e fornisce assistenza legale su questioni lavorative nazionali e internazionali, inclusi contenziosi relativi a discriminazione e molestie, norme sul personale e implementazione, contratti di assunzione e cessazione del rapporto di lavoro, riduzioni del personale, codici di condotta, questioni relative alla privacy, responsabilità sociale dell'azienda, protezione di informazioni riservate e segreti commerciali nonché delle conseguenze per la forza lavoro derivanti da acquisizioni e fusioni.

Cynthia Jackson è stata selezionata come uno dei "Best Lawyers in America" ed è stata ripetutamente nominata "Northern California Super Lawyer". Cynthia Jackson si è laureata con il massimo dei voti sia alla Stanford University che alla University of Texas School of Law.

Cynthia L. Jackson, Attorney at Law
Partner, Baker & McKenzie LLP
660 Hansen Way, Palo Alto, California 94304, USA
Tel +1 650-856-5572 Fax +1 650-856-9299
cynthia.l.jackson@bakernet.com

Sommario

Qual è il problema?

Archiviare, conservare, monitorare, filtrare e crittografare in maniera adeguata i dati elettronici non rappresenta più una scelta facoltativa, bensì un requisito irrinunciabile.

In un mondo in cui l'utilizzo dei dati elettronici sta crescendo rapidamente, le aziende devono trovare il modo di gestire i dati in maniera tale da poter controllare efficacemente i rischi posti dalla conformità normativa. La proliferazione dei dati elettronici è un fenomeno allo stesso tempo straordinario e travolgente. Considerata la quantità di spazio per l'archiviazione di cui dispongono i computer oggi in commercio, anche il più modesto negozietto a gestione familiare può avere una capacità di archiviazione elettronica pari a 2.000 armadi a quattro cassetti usati per gli schedari cartacei.[1] Il compito di gestire i dati elettronici è inoltre complicato dal fatto che i dati non sono più fogli di carta ma piuttosto byte di informazioni costantemente soggetti a modifiche, alterazioni e aggiornamento da parte di persone e fonti differenti. Archiviare, conservare, monitorare, filtrare e crittografare in maniera adeguata i dati elettronici non rappresenta più una scelta facoltativa, bensì un requisito irrinunciabile.

I sistemi elettronici controllano e dirigono macchinari, elaborano dati finanziari, gestiscono stock di magazzino, effettuano ordini e trasmettono immagini e documenti. Accrescono in maniera incommensurabile la velocità della comunicazione verbale e non verbale. L'email è la forma più familiare di comunicazione elettronica, ma altri componenti della comunicazione includono diari online ("web log" o "blog"), la messaggistica immediata (IM) in cui gli utenti chattano online in tempo reale, le webcam per la teleconferenza, i trasferimenti di documenti e video e i servizi voce a banda larga. Tali sistemi, tuttavia,

[1] Jason Krause, *E-Discovery Gets Real,* ABA JOURNAL, febbraio 2007; nota George L. Paul & Bruce H. Nearon, *The Discovery Revolution: A Guide to the E-Discovery Amendments to the Federal Rules of Civil Procedure,* ABA SECTION OF SCI & TECH. LAW.

Nel 2005, il 24% ha ricevuto la richiesta di presentare in giudizio messaggi email e il 15% ha sostenuto azioni legali avviate a causa del solo utilizzo dell'email da parte dei dipendenti.

possono essere soggetti a un utilizzo non corretto che può danneggiare un'azienda. Le persone possono infatti inviare messaggi intimidatori e molesti a dipendenti, manager e terze parti; possono scaricare ("rubare") proprietà intellettuale da aziende o terze parti, screditare l'azienda, e i suoi prodotti e servizi, clienti o concorrenti; oppure possono trasferire in segreto i dati sottratti fraudolentemente in località remote oppure archiviarli nella memoria fisica fornita dall'azienda. Gli utenti possono visualizzare o distribuire materiali che i tribunali possono avere giudicato come fonte di molestie o illegali, creare e pubblicare materiali diffamatori su siti Internet e blog e progettare o persino commettere crimini: tutto questo dal luogo di lavoro, utilizzando in maniera occulta le apparecchiature dell'azienda.[2]

Non c'è quindi da meravigliarsi se in un sondaggio condotto dall'Association of Corporate Counsel (ACC) l'86% dei giuristi d'impresa ha indicato come principale preoccupazione il "monitoraggio delle attività aziendali che possono avere implicazioni legali".[3] Nel 2005, il 24% delle aziende ha ricevuto la richiesta di presentare in giudizio messaggi email e il 15% ha sostenuto azioni legali avviate a causa del solo utilizzo dell'email da parte dei dipendenti. Secondo lo stesso sondaggio, il 10% dell'email sul luogo di lavoro presentava contenuti di tipo sessuale, sentimentale o pornografico.[4] Prima ancora che le norme di electronic discovery della Federal Rules of Civil Procedure (FRCP) entrassero in vigore il 1° dicembre

[2] *Electronic Workplace: Is Your Company's Work Blogging Down?* FEDERAL EMPLOYMENT LAW INSIDER, settembre 2006 in 2; Michael R. Phillips, *Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks,* Treasury Inspector General for Tax Administration, 31 luglio 2006.
[3] ACC & SERENGETI, MANAGING OUTSIDE COUNSEL SURVEY REPORT, 23 ottobre 2006.
[4] *2006 Workplace E-mail, Instant Messaging & Blog Survey: Bosses Battle Risk by Firing E-mail, IM & Blog Violators,* AMA, 11 luglio 2006, http://www.amanet.org/press/amanews/2006/blogs_2006.htm.
[5] AMA/ePolicyInstitute Research, *2004 Workplace E-mail and Instant Messaging Survey Summary,* in 1.

2006, più di un'azienda su cinque aveva ricevuto la richiesta di presentare le comunicazioni elettroniche nel corso di contenziosi o indagini governative nel 2004.[5] Questa percentuale è più che doppia in confronto al dato del 2001.[6] Di fatto, nel 2005 le aziende USA hanno speso 1,2 miliardi di dollari in servizi esterni di electronic discovery.[7] Questa cifra è stata stimata a 1,9 miliardi di dollari nel 2006.[8] Con l'entrata in vigore della normativa FRCP sull'electronic discovery, era ragionevole aspettarsi che tali statistiche sarebbero state ben presto obsolete. Sorprendentemente, tuttavia, in un sondaggio condotto a soli due mesi dalla data di entrata in vigore della normativa FRCP, solo il 7% degli uffici legali aziendali ha indicato che le proprie aziende erano preparate per le normativa emendata, mentre il 54% non sapeva nemmeno che la normativa sarebbe entrata in vigore a partire dal dicembre 2006.[9]

Nel 2005, le aziende USA hanno speso 1,2 miliardi di dollari inservizi esterni di electronic discovery. Questa cifra è stata stimata a 1,9 miliardi di dollari nel 2006.

Le aziende devono inoltre assicurare la conformità a un crescente numero di altre norme che disciplinano le comunicazioni elettroniche, e abbondano le nuove proposte di legge.[10] Gran parte della normativa riguarda la protezione di dati personali riservati, *ossia,* l'Electronic Communications Privacy Act del 1986[11]; l'Health Insurance Portability and Accountability Act del 1996[12]; il Children's Online Privacy Protection Act del 1998[13]; il Gramm-Leach-Bliley Act del 1999[14]; il Controlling the Assault of Non-Solicited Pornography and Marketing Act del 2003[15]; il California Security Breach Notification Act

[6] *Id.*
[7] Sacha Consulting, Ramon Nunez, Metal INCS, Gregory McCurdy, Microsoft Corp, ABA Digital Evidence Project, The National Law Journal/www. NLJ.com, 19 settembre 2005.
[8] *Id.*
[9] Sondaggio Lexis Nexis® Applied Discovery® effettuato presso l'ACC 2006 Annual Meeting, ottobre 2006.
[10] *Data Security: Federal and State Laws,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, 3 febbraio 2006; *Data Security: Federal Legislative Approaches,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, 9 febbraio 2006; *Obscenity and Indecency: Constitutional Principles and Federal Statutes,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, 25 giugno 2003.
[11] 18 U.S.C. § 101 *et seq.*
[12] 42 U.S.C. § 201 *et seq.*
[13] 15 U.S.C. § 6501 *et seq.*
[14] 15 U.S.C. §§ 6801-6809.
[15] 15 U.S.C. §§ 7701-7713.
[16] Cal. S.B. 1386 (2002) (Cal. Civ. Code §§ 1798.82 e parti di 1798.29).
[17] Cal. Civ. Code § 1798.81.5 (Cal. A.B. 1950 (2004)).
[18] Allan Holmes, *The Global State of Information Security 2006,* CIO MAGAZINE, 15 settembre 2006.

L'email indesiderata ammonta al 93% del totale della posta in entrata.

del 2002[16]; il California Security of Personal Information Act del 2004[17]; e numerose altre normative e disposizioni di legge nazionali e internazionali.[18]

In aggiunta alle normative che disciplinano la distruzione e la conservazione dei documenti, le aziende devono salvaguardarsi in misura sempre crescente dall'attività degli hacker e dalla perdita di preziosa proprietà intellettuale attraverso i mezzi elettronici.[19] Internet può esporre le risorse più preziose di un'azienda a terze parti. Nel 2004, l'email indesiderata ammontava al 73% del totale della posta in entrata; questa percentuale sale al 93% nel 2006.[20] La maggior parte di queste email non comportanto altro che fastidi o perdite di tempo, ma malware o contenuti nocivi quali virus, worm, downloader, trojan, spam, link spam, phishing e pharming mettono in pericolo la rete aziendale, nonché le informazioni commerciali e la proprietà intellettuale in essa residenti.[21] Eventuali hacker possono penetrare nella rete e accedere a segreti commerciali e informazioni riservate, sottrarre password e reindirizzare gli utenti a siti di download. Di tutti questi attacchi, il 33% viene segnalato come generato da utenti interni.[22]

Il 40% delle persone intervistate in un recente sondaggio del National Center for Supercomputing Applications (NCSA) ha dichiarato di visitare i siti di social networking dalla postazione di lavoro, esponendo in tal modo la rete della propria azienda ad attacchi da parte di hacker.[23] Il 68% delle aziende intervistate ha affermato di essere stata vittima di reati elettronici nel 2004; di queste aziende, il 43% ha segnalato l'accesso a informazioni, sistemi

[19] *Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth,* CRS REPORT FOR CONGRESS, 13 aprile 2005.
[20] AMA/ePolicy Institute Research, *2004 Workplace E-mail and Instant Messaging Survey* (2004); W*ireless Privacy and Spam: Issues for Congress,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, 22 dicembre 2004; *'Junk E-mail': An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam"),* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, 15 aprile 2003; *Cybercrooks Deliver Trouble,* WASHINGTON POST, 27 dicembre 2006, D1.
[21] *Pharming,* WEBSENSE, INC. (2006); *The Economic Impact of Cyber-Attacks*, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, 1° aprile 2004.
[22] Scott Berinato, *The Global State of Information Security 2005,* PRICE WATERHOUSECOOPERS AND CIO, 15 settembre 2005
[23] *CA/NCSA Social Networking Study Report,* RUSSELLRESEARCH.COM, in 4, http://staysafeonline.org/features/SocialNetworkingReport.ppt.
[24] *2005 E-Crime Watch Survey—Survey Results,* CSO MAGAZINE, U.S. SECRET SERVICE, CERT COORDINATION CENTER.,

o reti, mentre il 14% ha segnalato un furto di indirizzo IP.[24] In effetti, in documenti processuali recentemente resi pubblici, è stato reso noto che un direttore di laboratorio della DuPont aveva scaricato, nel corso di quasi cinque mesi, 22.000 documenti riservati, e aveva trasferito 180 documenti DuPont dapprima su un computer laptop e quindi presso il suo nuovo datore di lavoro. I documenti illustravano le principali tecnologie e linee di prodotti DuPont oltre a tecnologie nuove ed emergenti in fase di ricerca e sviluppo,," per un valore stimato di 400 milioni di dollari.[25]

>Anche attività legali o considerate "innocue" possono costare care e la tentazione di indulgere in tali condotte "innocue" è davvero grande. In un sondaggio del 2004 su 840 aziende USA, il 66% ha risposto che i propri dipendenti trascorrono ogni giorno fino a due ore al computer aziendale per scopi personali, il 24% da due a tre ore e un ulteriore 10% più di quattro ore.[26] Lo stesso sondaggio ha indicato che il 75% dei dipendenti ogni giorno invia o riceve fino a10 messaggi email personali.[27] Il 90% dei dipendenti trascorre fino a 90 minuti utilizzando la messaggeria immediata per scopi personali, il 19% include allegati ai messaggi di testo, il 16% distribuisce barzellette, pettegolezzi o commenti dispregiativi, il 9% invia informazioni riservate, e il 6% invia messaggi di testo sessuali, sentimentali o pornografici.[28]

Come conseguenza sia dei requisiti di legge obbligatori che delle best practice di protezione, le aziende devono individuare un programma di protezione, implementarlo

---

http://www.csoonline.com/info/ecrimesurvey05.pdf.
[25] David Kauffman, *How Safe Is Your Data?*, HR HERO LINE, 9 marzo 2007.
[26] AMA/ePolicy Institute Research, *2004 Workplace E-mail and Instant Messaging Survey* (2004).
[27] *Id.*
[28] *Id.*

e formare il personale *prima* che si verifichi una crisi di carattere legale. Poche aziende possono permettersi il lusso di pensare a questi problemi e affrontarli per la prima volta dopo avere intentato una causa, in questi casi la proprietà intellettuale risulta infatti già compromessa,," , le informazioni riservate sono state divulgate, oppure è stato creato un ambiente di lavoro ostile. Pianificare in anticipo è di importanza critica per un'organizzazione. Innanzitutto, le aziende devono pianificare la conservazione, l'archiviazione, e il monitoraggio delle comunicazioni. In secondo luogo, devono creare processi di crittografia e restrizioni di accesso appropriate. Infine, è necessario procedere alla formazione e all'auditing di processi e policy.

Chi si deve preoccupare?

La gestione dei dati elettronici coinvolge quasi tutto il personale di un'azienda: ufficio legale, responsabili per la conformità, auditor interni, reparto contabilità, responsabili IT, risorse umane e benefit, ufficio proprietà intellettuale e licenze, responsabili della supply chain, controllo esportazioni, reparto vendite e reparto commerciale.

Ad esempio, le società USA quotate in borsa sono soggette a numerosi obblighi di reporting, auditing e trasparenza come conseguenze della normativa Sarbanes-Oxley (SOX) e agli obblighi contabili e di archiviazione previsti dal Foreign Corrupt Practices Act. Le società impegnate in contenziosi in tribunali federali, o semplicemente "minacciate" di contenzioso, devono essere pronte a passare all'azione per proteggere i dati pertinenti archiviati elettronicamente. Le società del settore bancario e finanziario o sanitario sono soggette a normative e leggi dettagliate che disciplinano raccolta, utilizzo, accesso e distribuzione delle informazioni. Le società che operano sul mercato internazionale o che esportano prodotti hardware o software si troveranno obbligate a gestire i propri dati, inclusa la crittografia, secondo modalità complesse e a volte in conflitto.

Ma anche alle società non quotate in borsa, coinvolte in procedimenti legali in corso o semplicemente minacciate di contenzioso, operanti sul mercato internazionale o in settori disciplinati da normative particolari, l'era dei dati elettronici pone una serie di sfide. Gli studi hanno rilevato che un terzo dei furti di dati sono commessi da

Le aziende impegnate in contenziosi in tribunali federali, o semplicemente "minacciate" di contenzioso, devono essere pronte a passare all'azione per proteggere i dati pertinenti archiviati elettronicamente.

Nessuna azienda è immune. Le piccole e medie aziende devono pianificare in anticipo e implementare subito i sistemi.

dipendenti in servizio e che la stragrande maggioranza delle accuse legalmente rilevanti di diffamazione, discriminazione e molestie derivano dal comportamento di dipendenti *autorizzati*.[29] Nessuna azienda è immune. Le piccole e medie aziende devono inoltre pianificare in anticipo e implementare subito sistemi per salvaguardare la proprietà intellettuale dal furto,"proteggere i dipendenti da rivendicazioni legali relative a un ambiente di lavoro ostile oppure prepararsi per la sospensione delle procedure di distruzione dei documenti nel caso di minaccia di contenzioso.

Ironicamente, le stesse tecnologie che hanno creato tutte queste problematiche di proliferazione dei dati possono anche fornire la soluzione, attraverso sistemi di gestione dei dati elettronici correttamente progettate e gestite, personalizzate per soddisfare i requisiti di legge previsti dalla legislazione e dalle normative applicabili. Questi sistemi elettronici devono includere sistemi software dotati di funzionalità di conservazione e archiviazione dei documenti, funzionalità di sospensione delle procedure di distruzione dei documenti, restrizioni di accesso in crittografia quando richiesto, e funzionalità di monitoraggio e filtraggio web quando consentito. Oltre all'installazione di un tale sistema, è imperativo identificare gli appropriati parametri legali e formare il personale in previsione di un contenzioso legale, al fine di comprendere in che modo gestire in maniera appropriata e continuativa tali dati, ed essere in grado di acquisire e produrre i dati elettronici in maniera rapida, semplice e appropriata qualora se ne presenti la necessità dal punto di vista legale. La selezione e l'implementazione di sistemi di gestione dei dati elettronici, la creazione e l'applicazione di policy e la formazione e auditing continui del personale al fine

[29] Scott Berinato, *The Global State of Information Security 2005*, PRICE WATERHOUSECOOPERS AND CIO, 15 settembre 2005.

di assicurarsi che il sistema sia effettivamente funzionante *prima di un'eventuale azione legale*, richiedono la collaborazione coordinata e attenta del personale aziendale dell'ufficio legale, del reparto risorse umane e di tutti gli uffici coinvolti.

La selezione e l'implementazione di sistemi di gestione dei dati elettronici, la creazione e l'applicazione di policy e la formazione e auditing continui del personale al fine di assicurarsi che il sistema sia effettivamente funzionante *prima di un'eventuale azione legale*, richiedono la collaborazione coordinata e attenta del personale aziendale.

Requisiti legali per la gestione di documenti elettronici

Non conoscere gli emendamenti delle disposizioni federali di procedura civile può costare caro.

In assenza di una situazione di contenzioso," non vi è in genere alcun obbligo universale di conservare i dati archiviati elettronicamente (o altra documentazione), sebbene alcuni tipi di conservazione dei dati, ad esempio per fini fiscali, di impiego e aziendali possano essere richiesti in base alla legislazione federale o dei singoli stati. Una "situazione di contenzioso" d'altro canto innescherà obblighi di conservazione, richiedendo all'azienda di sospendere le normali procedure di distruzione dei documenti. I nuovi emendamenti all'FRCP codifica l'esigenza di una "sospensione per contenzioso" dei documenti che l'azienda ritiene ragionevolmente di dovere esibire in previsione di un contenzioso. La "sospensione per contenzioso" può essere attivata molto prima che venga effettivamente intentata una causa, ad esempio quando l'azienda riceve un reclamo interno rivolto a un "dirigente", una lettera cautelativa da una parte o da un legale che minaccia il ricorso alle vie legali, la corrispondenza della fase di precontenzioso, un avviso di garanzia da parte di un ente governativo, un mandato di comparizione o una richiesta di informazioni da parte delle autorità competenti o il deposito di un'accusa amministrativa. Una volta che si sia verificata una "situazione di contenzioso", l'azienda ha l'obbligo in base agli emendamenti di intraprendere misure esplicite al fine di sospendere immediatamente tutte le normali procedure di distruzione dei documenti e conservare tutta la documentazione, inclusi i dati in formato elettronico e i metadati in essi contenuti, che l'azienda

La società fu condannata al pagamento delle spese e delle spese legali dal ricorrente in quanto non aveva sospeso la distruzione di email e documenti e conservato documenti pertinenti a partire dalla data del *reclamo interno del dipendente* relativo a comportamenti di molestie sessuali.

sa o ragionevolmente dovrebbe sapere come rilevanti ai fini del procedimento legale o che abbia ritenuto possano condurre all'esibizione di prove ammissibili.

Anche prima dei recenti emendamenti all'FRCP, i tribunali hanno dimostrato scarsa comprensione nei confronti delle aziende che non avevano conservato i dati, pur sapendo o dovendo sapere dell'imminente azione legale. Nel giudizio *Broccoli contro Echostar Communications Corp,* 229 F.R.D. 506 (D.C. Md. 2005), la corte ha stabilito che il datore di lavoro aveva l'obbligo di conservare i documenti elettronici per gli 11 mesi precedenti alla cessazione del rapporto per opera del ricorrente/dipendente. Tale obbligo derivava dal fatto che il futuro querelante aveva notificato al suo datore di lavoro un reclamo verbale e scritto in merito a presunte molestie sessuali. La società fu condannata al pagamento delle spese e delle spese legali del querelante in quanto non aveva sospeso la distruzione di email e documenti e conservato documenti pertinenti a partire dalla data *del reclamo interno del dipendente* relativo a comportamenti di molestie sessuali.

In una serie di giudizi, *Zubulake contro UBS Warburg LLS,* 220 FRD 212 (S.D. N.Y. 2004), 229 F.R.D. 422 (S.D. N.Y. 20 luglio 2004 Zubulake II), e 231 FRD 159 (S.D.N.Y. 3 febbraio 2005 Zubulake III), la corte ha stabilito che l'azienda aveva l'obbligo di conservare i documenti elettronici per i quattro mesi precedenti alla presentazione di un'accusa di discriminazione da parte della ricorrente (e per 10 mesi prima che la ricorrente intentasse una causa in un tribunale federale), in quanto l'azienda sapeva o avrebbe dovuto sapere che le proprie

norme in merito alla distruzione dei documenti avrebbero avuto come esito la distruzione di documentazione rilevante ai fini del processo. Nel giudizio *Zubulake,* la corte aveva stabilito che i nastri di backup della rete del convenuto erano una probabile fonte di prove pertinenti, ma che i dipendenti esterni all'ufficio legale avevano provveduto a cancellare documentazione rilevante, che il convenuto ha successivamente recuperato mediante onerose attività di ripristino dei metadati.

Nel giudizio *Wiginton contro CB Richard Ellis,* 229 F.R.D. 568 (N.D. Ill. 2003), la corte ha stabilito che per l'azienda era da considerarsi notifica di "class action" la sola lettera del legale del ricorrente che identificava i documenti e più presunti molestatori alcuni giorni dopo che era stata intentata la causa. Specificamente, la corte riteneva che l'azienda avesse l'obbligo di conservare i dischi rigidi dei computer, gli account email e i dati Internet di tutti coloro accusati di molestie sessuali o in altro modo coinvolti nel caso. In aggiunta, la corte consentiva al ricorrente di rinnovare un'istanza sanzionatoria per la mancata conservazione dei dati elettronici relativi al ricorrente e dieci presunti molestatori, qualora i documenti elettronici mancanti venissero trovati nei nastri di backup dell'azienda. Nel giudizio *Consolidated Aluminum Corp contro Alcoa, Inc.,* 2006 U.S. Dist. LEXIS 66642 at *18 (M.D.La. 2006), la corte aveva ordinato ad Alcoa il pagamento delle spese per la nuova deposizione di tutti gli attori principali coinvolti e delle spese relative a procedimento e indagine di accertamento delle lacune dell'e-discovery, in quanto Alcoa aveva atteso circa due anni e mezzo dopo avere inviato la richiesta a Consolidated Aluminum

prima di sospendere la propria procedura di distruzione dei documenti. Nel giudizio *Samsung Elecs. Co. contro Rambus, Inc.,* 2006 U.S. Dist. LEXIS 50007 (E.D.Va. 2006), l'attore convenuto in via riconvenzionale Rambus aveva considerato il contenzioso identificando il più probabile obiettivo del contenzioso, i principi legali e i documenti pertinenti alla conservazione e distruzione prima di avere avviato la distruzione dei documenti. Avendo concluso che Rambus aveva impropriamente distrutto dati pertinenti, la corte aveva indicato l'imposizione di sanzioni di electronic discovery. Rambus aveva a sua volta volontariamente archiviato il reclamo riconvenzionale prima che la corte imponesse le sanzioni.

Le conseguenze del mancato annullamento delle procedure di distruzione dei dati e della mancata sospensione per il contenzioso sono significative. Nel giudizio *Zubulake,* la corte non solo aveva ordinato al convenuto di pagare i costi per la comunicazione degli atti, ma più significativamente aveva espresso alla giuria un pregiudizio negativo. Nello specifico, la corte aveva stabilito che la giuria poteva dedurre che i documenti distrutti avrebbero supportato i querelanti nell'accusa di discriminazione, in quanto i documenti non erano stati conservati dopo la data dell'accusa in base all'EEOC, presentata dieci mesi prima di qualsiasi procedimento legale. La giuria a sua volta condannò il convenuto al pagamento di 29 milioni dollari. Nel giudizio *Stati Uniti contro Philip Morris USA Inc.,* 327 F. Supp. 2d 21 (D.D.C. 2004), la corte condannò Phillip Morris al pagamento di 2.75 milioni di dollari sulla base di una

sanzione di 250.000 dollari, moltiplicata per gli undici manager responsabili della mancata conformità alle norme in materia di conservazione dei dati della società. In aggiunta, la corte precluse a tutti gli undici manager inadempienti la possibilità di deporre come testimoni della difesa al processo. Nel giudizio *Krumwiede contro Brighton Associates LLC,* 2006 U.S. Dist. LEXIS 31669 (N.D. Ill. 2006), la corte aveva pronunciato una sentenza di giudizio in contumacia quando il ricorrente/attore convenuto in via riconvenzionale aveva omesso di applicare una sospensione per contenzioso su un computer laptop e aveva continuato a accedere, eliminare, alterare. modificare i file prima di consegnare il laptop per la perizia legale, in quanto i metadati erano stati alterati attraverso l'utilizzo continuato anche se non risultavano completamente eliminati. Nel giudizio *Dempsey contro Pfizer,* 813 S.W. 2d 205 (1991), il tribunale del Texas aveva respinto una richiesta di 42.000.000 milioni di dollari come sanzione per la distruzione dei documenti.[30]

In aggiunta alle sanzioni pecuniarie, i tribunali hanno stabilito la responsabilità civile per la distruzione delle prove del giudizio e sanzioni penali.

In aggiunta alle sanzioni pecuniarie e alle indicazioni di pregiudizio negativo così significativamente dimostrate dai casi suddetti, i tribunali hanno anche imposto la responsabilità civile per la distruzione delle prove del giudizio e sanzioni penali. Frank Quattrone, un ex banchiere d'affari nel settore hi-tech presso il Credit Suisse First Boston è stato condannato all'interdizione permanente dal settore mobiliare e a una sanzione di 30.000 dollari dal NASD. In precedenza, Quattrone era stato condannato per avere ostacolato la giustizia con una sentenza di 18 mesi di reclusione con l'accusa di avere

[30] Né questi casi, tutti decisi prima degli emendamenti all'FRCP, sono da considerarsi stravaganti. Nel giudizio *In Re Quintus Corp. contro Avaya, Inc.* 2006 Bank.LEXIS 2912 (Bank. D. De. 2006), la corte ha emesso una sentenza di 1,88 milioni di dollari per la deliberata e pregiudiziale distruzione di prove che il convenuto era tenuto a conservare in conformità alla normativa e in previsione del contenzioso. Nel giudizio *In 3M Innovation Properties C. contro Tomar Electronics, Inc.,* 2006 U.S. Dist. LEXIS 80571 (D. Minn 2006), la corte ha espresso un pregiudizio negativo in quanto il convenuto non aveva istituito una sospensione per contenzioso. Nel giudizio *In Re Napster,* 462 F.Supp.2d 1060, 1077-78 (N.D. Cal. 2006), la mancata applicazione tempestiva di una sospensione per contenzioso ha causato l'emissione di un pregiudizio negativo da parte della corte. Nel giudizio *In Re NTL, Inc. Sec. Litig.* 2007 U.S. Dist LEXIS 9110 (S.D.N.Y. 2007), la corte ha stabilito che l'impresa appena costituita dopo la bancarotta non aveva conservato i documenti, con conseguente pregiudizio negativo e sanzioni pecuniarie. Nel dicembre 2006, la National Association of Securities Dealers (NASD) ha sostenuto che Morgan Stanley aveva falsamente dichiarato che milioni di messaggi email erano andati perduti in seguito agli attacchi al World Trade Center dell'11 settembre 2001. La causa è ancora pendente.

L'FRCP prevede l'obbligo per le parti avverse di discutere e cooperare reciprocamente in materia di dati elettronici fin dall'inizio del contenzioso e quindi per tutta la durata del procedimento.

inviato un messaggio email a membri del suo gruppo a proposito di "ripulire gli archivi" nel corso di un'indagine della SEC (la commissione di controllo di titoli e borsa statunitense).

Come dimostrato dai suddetti casi, l'FRCP codifica una materia sulla quale numerosi tribunali federali,[31] e alcuni tribunali statali hanno legiferato per alcuni anni. Ma gli emendamenti dell'FRCP influiscono anche sulle parti in causa in almeno altri due modi fondamentali: 1) esso disciplina espressamente l'electronic discovery e impone alle parti e ai rispettivi legali obblighi di ricerca, conservazione, presentazione e risposta in merito ai dati elettronici, eliminando ogni dubbio in merito alla rilevanza di tali dati; e 2) impone alle parti avverse di discutere e collaborare espressamente in relazione ai dati elettronici fin dall'inizio del contenzioso e quindi per tutta la durata del procedimento. Alle parti viene richiesto di incontrarsi ("meet and confer") in genere entro i primi mesi del contenzioso e concordare i dati da esibire, la forma in cui produrre tali dati elettronici (*ad esempio,* PDF, Tagged Image File Format (TIFF), formato "nativo", cartaceo, ecc.), eventuali affermazioni di inaccessibilità dei dati espresse da una delle parti," e concordare in che modo si intende sostenere eventuali oneri dovuti al recupero dei dati e gestire la divulgazione accidentale di informazioni di vario genere (ad esempio, dati relativi al rapporto avvocato-cliente, segreti commerciali o altro tipo di dati tutelati o protetti) eventualmente incorporate nei documenti elettronici o cartacei prodotti in base alla Rule 16 (b) e 26. A meno che le parti non abbiano implementato consapevolmente policy e procedure per la conservazione dei documenti prima che sia

[31] Nell'agosto 2006, una conferenza giudiziaria di magistrati statali ha approvato le *"Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information."* Queste linee guida, tuttavia, non sono vincolanti fino a quando non verranno adottate dai singoli Stati. A oggi, il Massachusetts e il North Carolina stanno considerando l'adozione di queste linee guida. Al contrario, il 1° settembre 2006, il New Jersey ha adottato una normativa sull'electronic discovery ispirata ai criteri dell'FRCP. Arizona, Florida, Idaho, Maryland e New Hampshire stanno considerando l'adozione di una normativa simile all'FRCP emendato. Il fatto che normative di electronic discovery simili ma differenti stiano emergendo tra gli Stati evidenzia ulteriormente la necessità che qualsiasi sistema di gestione di dati elettronici debba risultare sufficientemente versatile da rispondere sia alle regole generali che alle più sottili sfumature dell'electronic discovery.

intentata un'azione legale, la sessione "meet and confer" obbligatoria può rappresentare un serio svantaggio per le parti che non hanno programmato in anticipo tali procedure e che non sanno quali proposte possano risultare più vantaggiose.

Inoltre le disposizioni emendate disciplinano espressamente il ruolo dei dati elettronici nel caso in cui alle parti sia richiesto di rispondere a domande scritte (interrogatori) o di produrre fisicamente documenti. Ad esempio, FRCP 33 (d) consente alla parte rispondente di specificare che le informazioni di risposta si trovano in documenti commerciali, inclusi documenti archiviati elettronicamente, qualora (i) le risposte possano essere accertate sulla base di tali documenti, (ii) l'onere di accertamento delle informazioni sia essenzialmente il medesimo per entrambe le parti, e (iii) i documenti sono stati specificati. La sezione FRCP 34 emendata consente espressamente a una parte di specificare in che formato produrre i dati elettronici (in formato cartaceo o elettronico), sebbene per mancato accordo tra le parti o per ordinanza del tribunale, le disposizioni emendate presumono che i dati archiviati elettronicamente verranno prodotti nella forma in cui sono normalmente gestiti o in una forma ragionevolmente utilizzabile.

È prevedibile che la forma in cui devono essere prodotti i dati susciterà controversie per molti anni a venire. Alcuni hanno sostenuto che l'espressione "forma in cui sono normalmente gestiti",” richiederà la produzione di file di dati in formato "nativo". Altri obiettano perché la "forma nativa" non consentirà di rimuovere con facilità eventuali informazioni tutelate o protette oppure di controllare il

È prevedibile che la forma in cui devono essere prodotti i dati susciterà controversie per molti anni a venire.

numero di documenti prodotti. Alcuni tribunali e parti sostengono che i documenti devono essere prodotti con tutti i relativi metadati. *Williams contro Sprint/United Management Company,* 230 FRD 640 (D. Kan. 2005); *D.E. Tech contro Dell Inc.,* 2006 U.S. Dist. LEXIS 87902 (W.D. Va. 2006); *Nova Measuring Instruments contro Nanometrics Inc.* 2006 U.S. Dist. LEXIS 49156 (N.D. Cal. 2006); In *Re Payment Card Interchange Fee and Merchant Discount Antitrust Litigation,* 2007 U.S. Dist. LEXIS 2650 (E.D. N.Y. 2007). In maniera sempre crescente, tuttavia, i tribunali e altre parti sostengono che la presunzione dovrebbe essere sfavorevole alla produzione dei metadati. *Kentucky Speedway contro National Association of Stock Car Auto Racing Inc.,* 2006 U.S. Dist. LEXIS 92028 (E.D. Ky. 2006); *Wyeth contro Impax Laboratories Inc.,* 2006 U.S. Dist. LEXIS 79761 (D. Del. 2006); *The Ponka Tribe of Indians of Oklahoma contro Continental Carbon Co.,* 2006 U.S. Dist. LEXIS 74225 (W.D. Okla. 2006). In effetti, l'ABA ha emesso nel 2006 il parere formale 06-442 che affida al legale che invia i metadati potenzialmente protetti l'onere di eliminare i metadati o di inviare una differente versione del documento privo di metadati, al fine di eliminare la possibilità di produrre accidentalmente metadati tutelati o in altro modo protetti. L'ordine degli avvocati della Florida e quello del Maryland hanno imposto ai patrocinanti obblighi analoghi di filtraggio di metadati protetti prima di produrli in tribunale. Indipendentemente dalle decisioni di tribunali e gli ordini degli avvocati in merito ai metadati, una cosa è chiara: le aziende e i propri avvocati devono comprendere in che modo sono archiviati i dati elettronici e se in essi sono inclusi metadati, prima

di produrli, e prepararsi a queste problematiche ben in anticipo della sessione "meet and confer" obbligatoria del tribunale federale.

La disposizione emendata 37 prevede inoltre disposizioni di limitazione della responsabilità relativamente a sanzioni per la mancata produzione di dati archiviati elettronicamente, se tali dati vengono perduti in seguito a operazioni di routine di un sistema informativo elettronico e tali operazioni sono state eseguire in buona fede. Come notato in precedenza, tuttavia, è improbabile che un tribunale accetti tale buona fede, se una parte non impone tempestivamente una sospensione per contenzioso." Le problematiche della conservazione dei dati vanno al di là del server mainframe aziendale e riguardano nastri di backup, dischi rigidi, laptop e altri dispositivi di archiviazione elettronici. Questa materia non è così chiara come potrebbe sembrare a prima vista. L'azienda utilizza dispostivi PDA, come ad esempio il BlackBerry? Vi sono messaggi email memorizzati solo su tali dispositivi e non sui server aziendali? I dipendenti stampano e conservano copie cartacee di documenti anche se i file elettronici vengono periodicamente eliminati e si conosce dove sono conservate queste copie? Vi sono dipendenti che sul luogo di lavoro accedono a bacheche elettroniche, a programmi di messaggistica immediata o all'email personale? Il sistema aziendale di gestione dei documenti elettronici può avere conservato una copia di questi documenti? L'azienda tiene traccia della frequenza con cui vengono distrutti o sovrascritti i dati elettronici, e tali sistemi possono venire bloccati quando vengono ricercati specifici dati (quali nome, qualifica del potenziale ricorrente o i prodotti da lui acquistati)? L'azienda ha

Un sistema di gestione efficace deve risolvere ognuna di queste problematiche, in anticipo su un eventuale contenzioso, al fine di assicurarsi che una volta presentatasi la "situazione di contenzioso", l'azienda possa immediatamente identificare e preservare tutti i dati pertinenti in qualsiasi forma siano essi disponibili.

[32] Allen Smith, *Amended Federal Rules Define Duty to Preserve Work E-mails*, HR NEWS, 1° dicembre 2006.

comunicato con chiarezza le policy relative alle email che è possibile salvare nelle cartelle personali dei computer aziendali? Tali policy sono rispettate dai dipendenti? L'azienda è a conoscenza di quali metadati sono presenti sui suoi computer?

Un sistema di gestione efficace deve risolvere ognuna di queste problematiche, in anticipo su un eventuale contenzioso, al fine di assicurarsi che una volta presentatasi la "situazione di contenzioso", l'azienda possa immediatamente identificare e preservare tutti i dati pertinenti in qualsiasi forma siano essi disponibili.[32] I dati elettronici interessati dalla sospensione per contenzioso devono includere non solo i documenti creati dalla persona su cui si incentra il potenziale contenzioso, ma anche qualsiasi documento indirizzato o relativo a tale persona, e nel caso di azioni legali per discriminazione e class action, relativo ad altre eventuali persone in circostanze analoghe.

Ambiente di lavoro non ostile

Molti dei casi di molestie via email sarebbero stati evitati se fossero stati utilizzati filtri, in quanto l'email non sarebbe mai stata spedita.

Negli Stati Uniti,[33] è diventata opinione comune che applicare filtri e monitorare i dipendenti sia una best practice che consente di prevenire procedimenti legali per ambiente di lavoro ostile. "L'idea che i filtri siano necessari per evitare responsabilità legali sembra essere ormai universalmente accettata".[34] "Molti dei casi di molestie via email sarebbero stati evitati se fossero stati utilizzati filtri, in quanto l'email non sarebbe mai stata spedita".[35]

Come suggerito dalle statistiche e come dimostrato persino da una sommaria verifica dei casi di ambiente di lavoro ostile, i sistemi di posta elettronica sono stati la fonte di innumerevoli citazioni in giudizio per discriminazione e molestie. *EEOC v. Freddie Mac,* Civ. No. 97-1157-A, in 3-4 (E.D. Va. 24 luglio 1997) (procedimento intentato e pendente per almeno tre anni, relativo a messaggi elettronici offensivi per gli afroamericani che circolavano sul luogo di lavoro. Il datore di lavoro aveva l'obbligo di "prendere misure tempestive e risolutive".") *Olivant contro Dept. of Environmental Protection,* 1999 WL 430770 (N.J. Admin. 12 aprile) (la distribuzione di contenuti umoristici "sessisti" tramite il sistema di posta elettronica costituisce molestia sessuale); *Trout contro City of Akron* (Citazione No. CV-97-115879 (presentata il 17 novembre 1997); Verdetto, *id.* (15 dicembre 1998)); sentenza di 260.000 dollari nei confronti del comune di Akron perché i colleghi di lavoro guardavano materiale pornografico sui propri computer. Al contrario, nel giudizio *Delfino contro Agilent,* 145 Cal. App.4th 790 (6th Dist., 2006), la corte non ha ravvisato alcuna

[33] A livello internazionale, il monitoraggio è soggetto a varie restrizioni e proibizioni. Il presente documento si basa principalmente sul processo USA, sebbene, come indicato nella sezione VIII di seguito, per garantire la conformità con i numerosi requisiti delle varie giurisdizioni internazionali sia necessario un sistema di gestione dati più sofisticato.
[34] Eugene Volokh, Professor of Law UCLA, *Freedom of Speech, Cyberspace: Harassment Law and the Clinton Administration,* 63 LAW & CONTEMP. PROBS. 299 (2000).
[35] Wendy R. Leibowitz, *Avoiding E-mail Horror Stories: Policies and Filters the Best Defense,* N.Y. L.J., 15 dicembre 1998, in 5.

responsabilità dell'azienda per l'utilizzo da parte del dipendente dei computer del datore di lavoro al fine di inviare messaggi minacciosi su Internet, in quanto l'azienda ha preso misure tempestive non appena venuta a conoscenza di tale condotta. In aggiunta la normativa federale disciplina la pedopornografia, che viene considerata come "commercio clandestino"," rendendo quindi illegali la manipolazione, il possesso, la distribuzione, ecc., di tali materiali in base alla sezione 18 USC 2251 et al. L'azienda ha l'obbligo legale di segnalare immediatamente all'FBI qualsivoglia utilizzo di questi materiali di cui venga a conoscenza, pena la violazione della legge sulla pedopornografia.

Per difendersi e proteggersi da questi abusi, un numero crescente di aziende negli USA utilizza dispositivi di monitoraggio e filtri. Il mancato monitoraggio da parte di un datore di lavoro USA delle comunicazioni elettroniche in entrata e uscita nelle proprie apparecchiature può risultare in una grave responsabilità legale. Di conseguenza, i datori di lavoro USA devono comunicare ai propri dipendenti USA che i computer sono di proprietà del datore di lavoro, che sono disponibili per l'utilizzo aziendale, che le comunicazioni sono soggette in qualsiasi momento a monitoraggio, e che i dipendenti non devono aspettarsi privacy quando utilizzano un personal computer aziendale.[36]

Inoltre, i tribunali tendono sempre più a considerare il filtraggio come il mezzo meno restrittivo per proteggere le persone da contenuti offensivi distribuiti via Internet. Ad esempio, il 22 marzo 2007, un tribunale distrettuale della Pennsylvania ha dichiarato il Child Online Protection Act[37] come parzialmente incostituzionale in quanto i filtri erano un mezzo per impedire ai minori di

[36] *Monitoring Employee E-mail: Efficient Workplaces vs. Employee Privacy,* 2001 DUKE L. & TECH. REV. 0026 (2001).
[37] 47 U.S.C. § 231.
[38] *ACLU v. Gonzales*, No. 98-5591 (E.D. Pa. 22 marzo 2007).
[39] *Id.*

accedere a contenuti offensivi su Internet meno restrittivo di quanto il Congresso richiedeva per legge.[38] La corte ha ritenuto che i filtri generalmente bloccano circa il 95% del materiale sessualmente esplicito".[39] I filtri sono inoltre personalizzabili in base alle differenti età e alle differenti categorie verbali o possono essere completamente disattivati..."[40]

A fronte di normative, controversie e costi per errori evitabili sempre crescenti, le aziende utilizzano norme sul luogo di lavoro, in aggiunta alla tecnologia, per gestire la produttività, proteggere le risorse e incentivare il rispetto della conformità da parte dei dipendenti. Secondo quanto riportato, l'80% o più delle aziende USA informa i dipendenti del monitoraggio di contenuti, digitazioni di tasti e del tempo trascorso alla tastiera; il 76% controlla l'attività degli utenti sui siti web; il 65% blocca le connessioni a siti web non appropriati; l'82% comunica ai dipendenti che l'azienda archivia e analizza i file del computer; l'86% avvisa i dipendenti che viene eseguito il monitoraggio dell'email; e l'89% notifica ai dipendenti che l'utilizzo del Web viene monitorato.[41] Nel 2005, l'84% delle aziende USA aveva stabilito norme che disciplinavano l'utilizzo dell'email personale, l'81% prevedeva norme per l'utilizzo di Internet, il 42% aveva implementato norme relative alla messaggistica immediata personale, il 34% aveva disciplinato l'accesso ai siti web personali durante l'orario di lavoro, il 23% aveva implementato norme relative ai post personali sui blog aziendali, e il 20% delle norme aziendali limitava l'accesso ai blog personali durante l'orario di lavoro.[42] Nello stesso anno, il 26% dei datori di lavoro ha ammesso di avere licenziato dipendenti a causa dell'utilizzo non consentito di Internet e il 25% ha licenziato dipendenti per l'utilizzo non consentito dell'email.[43]

A fronte di normative, controversie e costi per errori evitabili sempre crescenti, le aziende utilizzano norme sul luogo di lavoro, in aggiunta alla tecnologia, per gestire la produttività, proteggere le risorse e incentivare il rispetto della conformità da parte dei dipendenti.

[40] *Id.*
[41] AMA/ePolicy Institute Research, *2005 Electronic Monitoring & Surveillance Survey,* (2005).
[42] *Id.*
[43] *Id.*

Proteggere la proprietà intellettuale è fondamentale per un'azienda di successo

Il volume dell'email cresce del 30% all'anno e l'email può contenere fino all'80% della proprietà intellettuale di un'azienda.

Il volume dell'email cresce del 30% all'anno, e l'email può contenere fino all'80% della proprietà intellettuale di un'azienda.[44] Un disastro non è più solo una possibilità teorica. Nel giudizio *Sonoco Products contro Johnson,* 23 P.3d 1287 (Co. App. 2001), la società ha ricevuto un risarcimento di quasi 7 milioni di dollari in un procedimento legale per appropriazione indebita, in cui un ex-dipendente e il suo nuovo datore di lavoro si erano accordati per utilizzare dati proprietari, fisici ed elettronici, di Sonoco sottratti da un dipendente.[45]

La corte ha ritenuto responsabile non solo il dipendente datosi alla latitanza con i dati elettronici, ma anche il nuovo datore di lavoro. Nel giudizio *Shurgard Storage contro Safeguard Self-Storage,* 119 F. Supp. 2d 1121 (W.D. Wash. 2000), il ricorrente ha intentato un procedimento legale contro un successivo datore di lavoro, in base al Computer Fraud and Abuse Act: un ex dipendente del ricorrente aveva utilizzato i computer del ricorrente per inviare via email informazioni di proprietà del ricorrente all'azienda convenuta, che ha quindi assunto il dipendente. Nel giudizio *Charles Schwab contro Carter,* 2005 U.S. LEXIS 21348, no. 04-C-7071 (N.D. Ill. 27 settembre 2005), la corte ha ritenuto che il ricorrente abbia patrocinato con successo la causa nei confronti del nuovo datore di lavoro di un ex dipendente in base al Computer Fraud and Abuse Act e al principio della responsabilità per le azioni dei subordinati. Mentre lavorava per il ricorrente Schwab, il dipendente aveva

[44] Frank Chambers, *EDD Tips for Email from the Front Line,* LAW TECHNOLOGY TODAY, marzo 2007.
[45] *Vedere anche, Sawyer v. Dept. of Air Force,* MSPB 1986, 31 MSPR 193; *US v. Middleton,* 35 F. Supp. 2d 1189 (N.D. Cal. 1999); *EF Cultural Travel BV v. Explorica Inc.,* 274 F.3d 577 (1st Cir. 2001); *Pacific Aerospace Electronics Inv. v. Taylor,* 295 F. Supp. 2d 1188 (E.D. Wa. 2003).

inviato via email informazioni di proprietà di Schwab al suo successivo datore di lavoro, Acorn. Schwab sosteneva che Acorn avesse richiesto al dipendente di accedere ai computer di Schwab senza autorizzazione.

Nel giudizio *Lowry's Reports contro Legg Mason,* 271 F. Supp. 2d 737 (D. Md. 2003), un dipendente aveva distribuito e ristampato materiale coperto da copyright sul luogo di lavoro. La corte aveva notato che era da considerarsi irrilevante il fatto che il datore di lavoro non fosse a conoscenza che il dipendente aveva continuato ad agire scorrettamente (dopo che il datore di lavoro aveva richiesto al dipendente di cessare la distribuzione del materiale coperto da copyright). La giuria emise un verdetto di 20 milioni di dollari.[46]

Ognuno di questi casi dimostra che se la società/vittima USA avesse monitorato le informazioni proprietarie in uscita e avesse bloccato o filtrato l'invio non autorizzato di tali informazioni, avrebbe evitato non solo anni di contenzioso ma anche e soprattutto la perdita di informazioni proprietarie. Dopo tutto, chiudere la stalla quando i buoi sono scappati è una soluzione che di rado ha successo, con o senza il conforto di un verdetto favorevole.

[46] La richiesta di un nuovo processo e giudizio su una questione di diritto sono stati negati nel giudizio *Lowry's Reports, Inc. contro Legg Mason, Inc.*, 302 F. Supp. 2d 455, 461 (D. Md. 2004).

Privacy: quando troppi dati sono un problema[47]

A differenza dei Paesi dell'Unione Europea (UE) e dei Paesi in altre aree geografiche del mondo, gli USA non prevedono un quadro normativo generale sulla privacy dei dati. Negli USA si tende piuttosto a risolvere le questioni legate alla privacy su base settoriale o industriale, con normative distinte relative alla creazione, conservazione, utilizzo e accesso ai dati personali coperti da privacy. In contrasto con l'attenzione alla conservazione dei dati espressa dall'FRCP, o alle lezioni sul monitoraggio indicate dai casi relativi ad ambienti ostili di lavoro, o ai casi relativi al Computer Fraud and Abuse Act, le leggi sulla privacy disciplinano e limitano i dati che un'azienda è in grado di raccogliere, elaborare, trasferire, conservare, utilizzare o distribuire. Di conseguenza, è importante che efficaci sistemi di gestione delle informazioni non solo abbiano la capacità di conservare e archiviare i dati quando necessario e di eseguire il monitoraggio all'interno degli USA, quando possibile, ma anche la capacità di restringere e limitare l'utilizzo e l'accesso a dati riservati consentito all'azienda per soli scopi espliciti e limitati.

Ad esempio, il Gramm-Leach-Bliley Act disciplina gli istituti finanziari, incluse società impegnate nel settore bancario, assicurativo, azionario e obbligazionario e nel settore della consulenza finanziaria e degli investimenti. La normativa fornisce protezioni limitate della privacy nei confronti della vendita di informazioni finanziarie private, codifica la protezione nei confronti del "pre-texting" (intercettazioni) teso a ottenere informazioni finanziarie

[47] Per ulteriori informazioni sulla privacy dei dati negli USA e nel mondo, vedere Baker & McKenzie *Global Privacy Handbook* (International Association of Privacy Professionals) ©2006.

L'HIPAA affronta la raccolta, l'utilizzo e l'accesso a dati sanitari per "enti coperti" definiti come programmi di assicurazione sanitaria, enti per la gestione di dati sanitari e fornitori di assistenza sanitaria che trasmettono dati sanitari.

private con l'inganno, e riconosce ai consumatori il diritto di non aderire alla condivisione limitata di "informazioni personali non pubbliche". Richiede inoltre agli istituti finanziari di gestire programmi di protezione delle informazioni rispondenti a criteri specificati dall'autorità normativa, quale la Federal Trade Commission's Standards for Safeguarding Customer Information.

Il Fair Credit Reporting Act (come altre normative statali analoghe) disciplina principalmente l'utilizzo e la divulgazione dei dati contenuti in "rapporti sui consumatori" realizzati da parte di società di fornitura di dati sui consumatori, cha hanno un'ampia definizione. Contiene limitazioni alla raccolta, utilizzo e divulgazione di procedimenti medici, finanziari e legali oltre a restrizioni speciali relative al furto di identità, rapporti sui consumatori per scopi di impiego lavorativo e "rapporti investigativi sui consumatori" con terze parti. Questa normativa contiene inoltre numerosi requisiti destinati alle società di fornitura di dati sui consumatori e agli utenti di tali rapporti, al fine di salvaguardare l'integrità dei dati e l'accuratezza dei dati raccolti e distribuiti, e requisiti per l'accesso a Internet, per l'utilizzo e per lo smaltimento sicuro delle informazioni derivate da tali rapporti sui consumatori.

L'Health Insurance Portability and Accountability Act (HIPAA) affronta la raccolta, l'utilizzo e l'accesso a dati sanitari per "enti coperti", definiti come programmi di assicurazione sanitaria, enti per la gestione di dati sanitari e fornitori di assistenza sanitaria che trasmettono dati sanitari. Le norme contenute nell'HIPAA disciplinano, tra le altre cose, l'utilizzo e la divulgazione di informazioni

sanitarie protette gestite in qualsiasi formato. Un ente coperto deve nominare un commissario per la protezione dei dati generalmente responsabile dell'implementazione e dell'applicazione delle norme e procedure previste dall'HIPAA e ha l'obbligo di conservare i dati per sei anni. Gli enti coperti devono inoltre assicurare la conformità al Security Standards for the Protection of Electronic Protected Health Information, 45 CFR 160 e 164. Nel gennaio 2007, il dipartimento di giustizia USA ha annunciato il primo caso di procedimento legale intentato in base all'HIPAA, riguardante il furto di dati identificativi sanitari che includeva 1.130 documenti elettronici sottratti dalla Cleveland Clinic. Un dipendente avrebbe utilizzato i computer della clinica per raccogliere e vendere le schede dei pazienti a un gruppo criminale organizzato che aveva quindi utilizzato tali dati per fatturare fraudolentemente a Medicare 7 milioni di dollari. I dati sanitari sono disciplinati e controllati da diverse leggi statali quali il Confidentiality of Medical Information Act della California.[48]

Le norme contenute nell'HIPA disciplinano, tra le altre cose, l'utilizzo e la divulgazione di informazioni sanitarie protette gestite in qualsiasi formato.

Numerosi Stati hanno inoltre statuti espliciti che proteggono la riservatezza dei numeri di previdenza sociale. Ad esempio, la sezione 1798.85 del codice civile della California, proibisce, tra le altre cose, di richiedere a un cittadino di trasmettere via Internet il proprio numero di previdenza sociale, se la connessione non è protetta o se il numero di previdenza sociale non è crittografato. La sezione 1798.81.5 del codice civile della California richiede alle aziende di applicare ragionevoli procedure di sicurezza al fine di proteggere un'ampia gamma di dati personali, inclusi i numeri di previdenza sociale, i numeri di carte di credito e conti bancari,

[48] In un recente sondaggio, il 98,5% degli intervistati ha dichiarato di ritenere che le organizzazioni sanitarie abbiano la responsabilità di proteggere le cartelle sanitarie dei pazienti, ma meno del 40% si è dichiarato fiducioso che i propri fornitori di servizi sanitari proteggano effettivamente i dati sanitari personali. In pratica, tutti gli intervistati hanno risposto di ritenere che le organizzazioni sanitarie abbiano la responsabilità legale di avvisare i pazienti qualora si verifichi un accesso ai dati senza il consenso del paziente, tuttavia 7 intervistati su 10 non ritenevano che i fornitori di assistenza sanitaria applicassero la necessaria diligenza nell'informare i pazienti di sospette violazioni della privacy dei dati. www.epictide.com.
[49] NY CLS Gen. Bus. §399-h (2007).

La violazione delle normative USA federali e statali in materia di privacy dei dati non solo comporta una responsabilità penale ma inficia anche l'integrità di un'azienda e del suo marchio. Ancora una volta, pianificare in anticipo per evitare la violazione risulta di gran lunga preferibile a tentare semplicemente di riparare il danno una volta che esso si è verificato.

i numeri delle patenti di guida e altri tipi di dati. Lo stato di New York ha una legislazione simile che disciplina la distruzione dei documenti contenenti dati personali, quali il numero di previdenza sociale.[49]

Le aziende devono selezionare con attenzione i sistemi di gestione dei dati elettronici al fine di rispondere ai diversi e sempre più stringenti requisiti di protezione della privacy dei dati. Il medico e il bancario hanno entrambi necessità di funzionalità di crittografia per assicurarsi che i dati riservati, siano essi diagnostici o finanziari, siano salvaguardati dalla divulgazione accidentale. È necessario installare firewall e prevedere limitazioni di accesso per impedire la distribuzione troppo ampia o non autorizzata di tali dati. Deve essere disponibile una funzionalità di monitoraggio che, qualora venga rilevata una violazione della protezione, consenta di notificare in maniera appropriata la violazione e di prendere immediatamente le necessarie misure correttive. La violazione delle normative USA federali e statali in materia di privacy dei dati non solo comporta una responsabilità penale ma inficia anche l'integrità di un'azienda e del suo marchio. Ancora una volta, pianificare in anticipo per evitare la violazione risulta di gran lunga preferibile a tentare semplicemente di riparare il danno una volta che esso si è verificato.

Crittografia

La crittografia è una tecnologia indispensabile, sebbene ancora troppo spesso sottoutilizzata. Con crittografia dei dati si definisce il processo di codifica delle informazioni trasmesse o memorizzate al fino di renderle incomprensibili fino a quando non vengono decriptate dal destinatario a cui sono indirizzate.[50] La crittografia è di importanza fondamentale per proteggere i segreti commerciali e le informazioni riservate trasmessi via Internet.

Se non dispone di funzionalità di crittografia, un'azienda rende accessibili a tutti i propri segreti commerciali e industriali. "Nel mondo della sicurezza, il 2005 sarà ricordato come l'anno in cui la fuga di dati ha conquistato le prime pagine dei giornali, principalmente sull'onda delle nuove normative USA che precedono la divulgazione pubblica di casi di sottrazione o fuga di dati relativi a clienti".[51] Quello che spaventa ancora di più è che i dipendenti con accesso ai dati riservati del proprio datore di lavoro o non danno priorità alla protezione dei dati o non hanno familiarità con le modalità di utilizzo di tali dati. Nel fondamentale articolo, “Why Johnny Can’t Encrypt,”[52] due ricercatori della Carnegie Mellon University hanno scoperto che l'utente medio avanzato dell'email non sa in che modo utilizzare la tecnologia di crittografia. Lo studio che ne è derivato, "Why Johnny Still Can’t Encrypt"[53] ha rilevato un leggero miglioramento della situazione. È necessario che le società prendano misure propositive al fine di acquisire sistemi di crittografia intuitivi e di facile utilizzo che soddisfino le

[50] Fred Moore, *Preparing for Encryption: New Threats, Legal Requirements Boost Need for Encrypted Data,* COMPUTER TECHNOLOGY REVIEW, agosto-settembre 2005.
[51] Kevin Murphy, *Email Security Uncovered,* COMPUTER BUSINESS REVIEW ONLINE, 1° novembre 2005 (cita Alex Hernandez, direttore sviluppo prodotti avanzati di CipherTrust).
[52] Alma Whitten & J.D. Tygar, *Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0,* disponibile in http://www.gaudior.net/alma/johnny.pdf.
[53] Steve Sheng et al, *Why Johnny Still Can’t Encrypt: Evaluating the Usability of Email Encryption Software,* disponibile in http://cups.cs.cmu.edu/soups/2006/posters/sheng-poster_abstract.pdf.

Dal momento che gli hacker sanno che le aziende di fascia media di mercato spendono in genere meno per la protezione e la crittografia, si stima che oltre 4.000 aziende risultino vulnerabili nei confronti di attacchi se non implementano un programma di protezione dei dati.

esigenze di sicurezza degli utenti, per poi fornire agli utenti il necessario training sull'utilizzo di questa tecnologia.

I sistemi di archiviazione dei dati che memorizzano informazioni non crittografate espongono le aziende al rischio di furto dei dati dei propri clienti da parte degli hacker, con potenziali danni alle pubbliche relazioni, perdita di clienti e contenziosi economicamente onerosi. Ad esempio, nel gennaio 2007 le società della TJX, un gruppo di società che T.J. Maxx, Marshalls, Home Goods, Bob's Stores e altre catene di vendita al dettaglio, hanno annunciato che i propri sistemi informatici erano stati violati da hacker fin dal 2005-2006, con il conseguente furto dei dati relativi a 45,7 milioni di carte di credito distinte utilizzate dal 2002 al 2004, inclusi i nomi dei titolati e i numeri di carte di credito e di debito.[54] Nel marzo 2007, Radioshack ha appreso che 20 scatoloni contenenti documenti inviati al macero contenevano scontrini che riportavano i numeri di carta di credito dei clienti. Il procuratore generale del Texas ha avviato un'azione esecutiva. Nel marzo 2007, Group Heath Cooperative Healthcare System ha perso due laptop aziendali contenenti nomi, indirizzi, numeri di previdenza sociale e identificativi sanitari di pazienti e dipendenti locali.

L'utilizzo della crittografia avrebbe consentito di evitare ognuno di questi due incidenti. Le aziende di fascia media possono essere particolarmente vulnerabili gli attacchi. Gli hacker non desiderano più diventare famosi per avere creato un virus che si è diffuso a livello mondiale. Al contrario, vogliono fare soldi. Dal momento che gli hacker sanno che le aziende di fascia media di

[54] TJX, Frequently Asked Questions, www.tjx.com/tjx_faq.htm.
[55] Allan Holmes, *Many Mid-Market Enterprises Say They Have Neither the Time, Money nor Resources to Spend on Security. Which May Be Why the Crooks Are Targeting Them and Turning the Mid-Market into a Bad Neighborhood*, CIO, 1° marzo 2007.

mercato spendono in genere meno per la protezione e la crittografia, si stima che oltre 4.000 aziende risultino vulnerabili nei confronti di attacchi se non implementano un programma di protezione dei dati.[55]

Come in precedenza indicato, la crittografia viene considerata una protezione efficace nei confronti della pubblicazione accidentale dei dati almeno nel Confidentiality of Social Security Number Act della California.[56] Sono inoltre richiesti diversi standard di crittografia ai fornitori governativi nel settore dell'intelligence.[57] In più, è semplice buon senso utilizzare la crittografia per evitare la divulgazione accidentale di informazioni proprietarie. I reparti IT e gli uffici legali devono coordinare il fabbisogno aziendale di servizi di crittografia e determinare se il sistema corrente fornisce la protezione necessaria in caso di attacco di hacker, furto di dati o procedimento legale.

[56] CAL. CIV. CODE §1798.29 (parte della normativa conosciuta anche come SB 1386).
[57] National Institute of Standards and Technology (NIST), Data Encryption Standard Fact Sheet, in http://csrc.nist.gov/cryptval/des/des.txt.

Questioni internazionali: quando diverse concezioni di conformità dei dati entrano in conflitto

Le normative relative a raccolta, elaborazione, conservazione, utilizzo, monitoraggio, accesso e distruzione dei dati non solo differiscono in maniera significativa nella giurisdizioni al di fuori degli USA, ma in alcuni casi, contraddicono frontalmente la legislazione USA. Per le aziende che operano sul mercato internazionale, risulta pertanto di importanza essenziale comprendere sia la conformità nazionale che le normative estere applicabili ai dati elettronici.

Per le aziende che operano sul mercato internazionale, risulta pertanto di importanza essenziale comprendere sia la conformità nazionale che le normative estere applicabili ai dati elettronici.

Nell'Unione Europea, ad esempio, ogni Paese ha, conformemente alla direttiva dell'UE sulla privacy dei dati, implementato normative che disciplinano raccolta, registrazione, organizzazione, archiviazione, adattamento, alterazione, recupero, blocco, monitoraggio, utilizzo, divulgazione, trasmissione, trasferimento e distruzione dei dati di identificazione personale, e in alcuni casi sono previste ulteriori protezioni per i dati di identificazione personale riservati. A differenza degli USA, i dati di identificazione personale nell'Unione Europea hanno un'ampia definizione, e in genere non sono limitati da settore e industria, ma piuttosto viene protetta l'elaborazione o la trasmissione dei dati personali quali nome, indirizzo, retribuzione, benefit e informazioni finanziarie oltre che di dati maggiormente riservati riguardanti la salute, l'etnia o la razza, l'affiliazione politica o sindacale o lo stato civile. Tali normative si estendono non solo ai dipendenti ma anche ai consumatori. L'Italia, l'Austria e altri Paesi non si

Le aziende hanno necessità non solo di comprendere quali tipi di dati è consentito raccogliere, elaborare e trasmettere a livello internazionale, ma devono anche fare i conti con normative concorrenti e a volte in conflitto.

limitano a proteggere la privacy dei dati delle persone ma estendono la protezione della privacy dei dati anche alle aziende.

Dal momento che gli USA sono fondamentalmente considerati come una giurisdizione "non sicura" da parte dell'Unione Europea, tali dati non possono venire legalmente trasferiti, elettronicamente o in altro modo, negli USA o in altre "giurisdizioni non sicure", a meno che non siano previsti meccanismi di salvaguardia quali l'accordo USA-UE Safe Harbor, l'adozione dei modelli di clausola dell'UE oppure l'implementazione di norme approvate sulla privacy dei dati. Anche quando sono previste tali protezioni per consentire il trasferimento di dati di identificazione personale negli USA, può non essere consentito l'ulteriore trasferimento di tali dati verso processori terzi non identificati, o verso altri Paesi, ad esempio verso i servizi di data entry in India. I Paesi dell'UE sono in buona compagnia: Canada, Argentina, Giappone, Australia e molti altri Paesi stanno adottando diversi livelli di protezione della privacy dei dati.

Le aziende hanno necessità non solo di comprendere quali tipi di dati è consentito raccogliere, elaborare e trasmettere a livello internazionale, ma devono anche fare i conti con normative concorrenti e a volte in conflitto. Ad esempio, SOX richiede che le società quotate in borsa abbiano una linea diretta anonima cui segnalare sospette violazioni relative al settore finanziario e mobiliare. L'obiettivo della linea diretta anonima SOX è assicurare ai dipendenti l'anonimato ed evitare eventuali ripercussioni. Al contrario, l'Unione Europea in genere non apprezza le linee dirette anonime, in quanto le considera una violazione della privacy, e limita pertanto le segnalazioni

anonime. L'attenzione di SOX alla trasparenza in confronto alla preoccupazione per la privacy dell'UE pone un ovvio dilemma per le multinazionali quotate in borsa, e richiede un sofisticato sistema di gestione dati per assicurarsi che, tra le altre cose, vengano salvaguardati la conservazione, l'accesso e il recupero appropriati e limitati, soddisfacendo allo stesso tempo i requisiti SOX degli USA.[58]

Altre best practice statunitensi semplicemente non possono venire tradotte a livello internazionale. Ad esempio, nel 2001 la Corte suprema francese ha ritenuto che il licenziamento di un dipendente francese da parte di un'azienda francese, che aveva appreso dal monitoraggio del computer aziendale che il dipendente aveva inviato informazioni riservate a un potenziale concorrente, rappresentasse non solo un licenziamento senza giusta causa ma anche una violazione penalmente rilevante e incostituzionale. Il tribunale francese ha ritenuto che il dipendente aveva il diritto costituzionale alla privacy durante l'orario lavorativo e sul luogo di lavoro, anche se il datore di lavoro aveva vietato l'utilizzo del computer aziendale per scopi non attinenti all'attività lavorativa. La Germania ha posizioni leggermente più sfumate, ma limita anch'essa il monitoraggio dei computer dei dipendenti se il datore di lavoro consente al dipendente di utilizzare il computer per scopi personali. Diverse giurisdizioni dell'UE richiedono che qualsiasi monitoraggio dei dipendenti sia come minimo registrato e autorizzato dalla locale authority per la privacy dei dati.

Risulta pertanto imperativo che quando si seleziona un sistema di gestione dati elettronico l'azienda comprenda i requisiti di legge locali del Paese in cui avviene la

[58] Per un'ulteriore discussione su codici di condotta eccessivamente normativi e sovrautilizzazione di linee dirette anonime, vedere *"Overreaching Global Codes of Conduct Can Violate the Law"*, di Cynthia L. Jackson, LA e SF Daily Journal, giugno 7, 2006.

raccolta, l'utilizzo o l'accesso ai dati. Se, come nel caso di multinazionali, i dati hanno origine o sono trasferiti in più giurisdizioni, è di importanza critica rispettare le normative sulla privacy e che siano presenti firewall appropriati e restrizioni di accesso in ogni sistema dati, al fine di impedire l'elaborazione, il monitoraggio o il trasferimento dei dati in assenza di misure di salvaguardia appropriate e conformi.

Suggerimenti per le best practice

1. **Pianificare in anticipo.** Non attendere le denunce o le proteste di un ambiente di lavoro ostile, la divulgazione di segreti commerciali o la perdita di informazioni riservate per implementare un piano di gestione dei dati.

2. **Accertarsi di quali sono gli obblighi di legge.** Comprendere i requisiti di legge per il settore in cui si opera e le normative dei Paesi in cui opera l'azienda. Ad esempio, quali sono gli obblighi di conservazione dei dati per un dato tipo di informazioni in un dato Paese o Stato? Quali eventuali forme di tutela esistono per limitare l'accesso o gli obblighi di conservazione? Conoscere ciò che deve essere crittografato e quali obblighi di notifica esistono nel caso si verifichi una violazione della sicurezza? In una determinata giurisdizione i filtri sono una scelta prudente al fine di evitare che si crei un ambiente di lavoro ostile oppure vengono considerati una violazione della privacy?

3. **La stessa taglia non va bene per tutti.** Se si opera a livello nazionale o internazionale, capire quali sono gli obblighi, a volte in conflitto tra loro, a cui i sistemi per la gestione dei dati elettronici devono sottostare. Prendere in considerazione firewall, restrizioni di accesso e la disattivazione di determinate funzioni in alcune giurisdizioni che, ad esempio non consentono il monitoraggio o l'utilizzo di filtri.

4. **Assegnare le responsabilità per la gestione del sistema.** Assegnare a membri del personale la responsabilità per la conservazione e la gestione dei dati elettronici. Potrebbe trattarsi di un gruppo di persone composto da rappresentanti del reparto IT e dell'ufficio legale, che si avvalgono di suggerimenti

del reparto risorse umane e di altre reparti. Coinvolgere fin dall'inizio le persone che dovranno far funzionare il sistema nel caso si presentino richieste dovute a contenziosi legali.

5. **Individuare le varie forme in cui vengono conservati i dati e chi ne è il custode.** Ricordare che i dati possono essere memorizzati in una scrivania, in un PDA (Personal Digital Assistant), un computer desktop, un portatile e altrove. Prima di poter gestire dati per i quali la legge ritiene responsabile l'azienda, è innanzitutto necessario individuare quali sono e dove si trovano per garantire che i sistemi utilizzati, acquisiscano effettivamente i dati pertinenti. Conoscere i metadati di cui si è in possesso.

6. **Selezionare un sistema di gestione dati flessibile.** Selezionare un sistema sufficientemente flessibile da rispondere alle specifiche esigenze aziendali di conservazione, archiviazione, monitoraggio, filtraggio e crittografia dei dati nelle giurisdizioni in cui opera l'azienda. Scegliere un sistema intuitivo e facile da usare per assicurarsi che venga regolarmente utilizzato dagli utenti. Scegliere un sistema in grado di adeguarsi a requisiti legali in evoluzione. Pianificare la crescita e la proliferazione dei dati, metadati inclusi.

7. **Non esagerare.** Solo perché la tecnologia consente di memorizzare enormi quantità di dati ciò non significa che si debba farlo per forza. La memorizzazione di dati inutili non solo complica il recupero dei dati ma può anche aumentare i rischi di hacking. Ad esempio, non conservare dati finanziari riservati dei clienti a meno che non se ne abbia effettivamente bisogno. In tal caso, conservarli in forma crittografata.

8. **Adottare policy.** Adottare policy chiare e semplici, coerenti con la normativa in vigore che disciplina la conservazione dei documenti, inclusa una tempestiva

sospensione per contenzioso. Negli USA, adottare una policy di monitoraggio dell'email dei dipendenti ampiamente pubblicizzata. Adottare policy di crittografia per le informazioni riservate per evitarne la divulgazione accidentale. Dove consentito, adottare procedure disciplinari per lanciare un segnale forte al personale.

9. **Prepararsi.** Non attendere che si verifichi una situazione di contenzioso (per non parlare di un procedimento legale) per implementare una procedura di sospensione per contenzioso. Creare subito la procedura di sospensione della distruzione dei documenti, in maniera tale che se necessario sia possibile attivare rapidamente la sospensione per contenzioso. Prepararsi preventivamente a qualsiasi sessione "meet and confer" relativa all'electronic discovery. La parte in causa che sa di quali dati è in possesso e del motivo di tale possesso si troverà in una posizione di vantaggio e potrà negoziare il programma di electronic discovery più favorevole. Non attendere che si verifichi una violazione della protezione per implementare procedure di notifica e rapporto tempestivi.

10. **Formazione e auditing continui.** Una policy e un sistema di gestione dei dati funzionano solo se i dipendenti sanno come utilizzarli. Essi richiedono un'implementazione e una manutenzione scrupolosa e regolare. L'acquisto di un sistema di gestione dati rappresenta solo il primo passo verso la conformità. Nuovi dati, nuove tecnologie, nuove normative, nuove minacce e nuovi dipendenti richiedono tutti una attenzione e attività continue di training e auditing.

WP33-0705