

ISACAROMA Newsletter

Privacy e protezione dei dati personali - intervista a Francesco Amendola

A due anni dall'entrata in vigore della nuova normativa sulla *privacy* quale bilancio possiamo tracciare?

In realtà è bene ricordare che la normativa sulla *privacy* o, per essere più corretti, sulla protezione dei dati personali, esiste in Italia dal 1997, a seguito dell'entrata in vigore della legge 675/96.

Il D.Lgs. 196 del 30 Giugno 2003, abrogando e sostituendo tutte le leggi, i decreti ed i regolamenti previgenti nel medesimo ambito di applicazione, ad eccezione delle disposizioni di legge e di regolamento più restrittive, ha riunito in un testo unico l'intera normativa in materia di *privacy*, razionalizzandola ed armonizzandola; inoltre ha introdotto nuove garanzie per i cittadini ed ha modificato e semplificato alcune procedure, così da rendere questa materia, tutt'altro che semplice, di più immediata applicazione nel contesto italiano.

Questa premessa per ricordare anzitutto che molti degli adempimenti ad oggi non ancora posti in essere in numerose realtà (es. informativa all'interessato all'atto dell'acquisizione dei dati circa le modalità e le finalità del trattamento, adozione di alcune misure minime di sicurezza, notifica al Garante dell'avvio di una banca dati, etc.) sono in realtà obbligatori già da qualche anno. A questa situazione di scarsa sensibilizzazione e sfiducia verso la tutela dei dati personali, sia da parte dei titolari dei trattamenti che da parte degli interessati, si aggiungono i continui rinvii dell'obbligo di adozione degli articoli del nuovo codice *privacy* relativi alle misure minime di sicurezza: sebbene l'intento originario di tali rinvii sia stato quello di concedere un lasso di tempo maggiore per adeguarsi agli adempimenti del decreto, il continuo posticipo della data ultima di adeguamento ha accentuato il disinteresse verso l'effettiva applicazione del codice *privacy*. In aggiunta vi è stata anche una scarsa o errata informazione da parte dei media che, ben solerti su altre tematiche, hanno messo in secondo piano le notizie su questa materia e talvolta la stessa Autorità Garante è stata contraddittoria nei suoi comunicati. Il risultato è che si può ingenerare confusione tra i destinatari del D.Lgs. 196/03: ad esempio non sempre si ha la consapevolezza che le disposizioni transitorie riguardano solo l'adozione delle misure

minime di sicurezza non previste dal D.P.R. 318/99, credendo a volte erroneamente che la proroga riguardi l'applicazione dell'intero codice.

Inoltre, l'attività ispettiva, di controllo e sanzionatoria da parte dell'Autorità Garante, sebbene in progressivo aumento anche a seguito del recente protocollo d'intesa con la Guardia di Finanza, non ha ancora raggiunto l'efficienza necessaria per incidere significativamente sulla percezione che di essa ne hanno titolari ed interessati di trattamenti. Spesso infatti il comune sentire dei primi è ancora riluttante a considerare di per sé precettive le parti del D.Lgs. 196/03 già in vigore, a volte addirittura ponendole in contrasto con altri adempimenti normativi e dunque rifiutandole; viceversa gli interessati da trattamenti non ritengono ancora di avere sufficienti garanzie che vi sia il rispetto delle norme da parte dei titolari che trattano i loro dati e ne scelgono insindacabilmente gli strumenti e le modalità di trattamento.

Tirando dunque le somme, si delinea uno scenario non proprio rasserenante in cui emergono fenomeni: di superficialità nel trattamento dei dati da parte dei titolari che spesso non si preoccupano di adottare idonee misure di sicurezza; di abuso, qualora si voglia celare dietro la *privacy* l'incapacità o la mancanza di volontà di fornire le informazioni richieste; infine di sfiducia nel sistema di protezione di dati personali da parte dei cittadini interessati da trattamenti, che a volte associano al termine *privacy* il concetto di silenzio o addirittura di "omertà" da parte dell'istituzione che non può fornire i dati richiesti, piuttosto che di tutela della riservatezza degli stessi.

Si parla sempre di *privacy* ma in realtà il D.Lgs. 196/03 introduce una serie di nuovi diritti per ogni cittadino: diritto alla riservatezza, all'identità personale, alla protezione dei propri dati personali. Che impatto ha avuto ed avrà questa legge?

Nell'ambito della sicurezza delle informazioni i beni immateriali da proteggere sono la riservatezza, l'integrità e la disponibilità dei dati. Il nuovo codice *privacy* recepisce questi principi e li adotta nel momento in cui chiarisce le proprie finalità in termini di garanzia che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Si gettano le basi così per una società dell'uguaglianza, della partecipazione, della libertà e soprattutto della dignità, cioè per una società in cui questi valori, ai quali si aggiunge la *privacy*, sono profondamente legati tra di loro.

Ciò che però accade è che si confonde troppo spesso il termine *privacy* nell'accezione data dal nostro ordinamento - "*diritto alla protezione dei dati personali*" - con il significato originario della parola, di provenienza anglosassone, ovvero "*right to be let alone*", il diritto di essere lasciato solo.

Questa discrasia non ha certo contribuito a far comprendere ai titolari dei trattamenti di dati in cosa siano tutelati dal D.Lgs. 196/03, generando per contrappunto la preoccupazione di violare continuamente la normativa ad ogni scambio di informazioni e, dunque, portandoli ad adottare la filosofia del "meglio non fornirle affatto", piuttosto che rischiare di fornirle oltre misura. Allo stato attuale la percezione che si ha è che tutto il sistema di tutela della protezione dei dati personali sia solo un insieme di meri adempimenti formali da attuare onde evitare sanzioni, tra l'altro in apparente contraddizione con altri sistemi di garanzia dei diritti dei cittadini interessati da trattamenti, quali ad esempio i codici di deontologia degli ordini professionali. Questo conflitto, ad esempio, ha portato gli avvocati a ritenere di non dover essere annoverati tra i destinatari del D.Lgs. 196/03, in quanto già tenuti professionalmente alla riservatezza dei dati trattati, tanto da farsi promotori di una legge in cui formalmente la categoria viene sollevata da tutti gli adempimenti previsti dal codice.

Analogamente un atteggiamento diffuso tra i titolari è quello per cui nell'analizzare il trattamento di dati effettuati, per verificarne la conformità a quanto previsto dal codice, si cerca spesso di trovare le motivazioni idonee ad escludere il maggior numero di adempimenti possibili, piuttosto che valutare in modo puntuale e compiuto la natura, le modalità e le finalità, oltre che le possibili criticità, dei trattamenti stessi; tutto questo accade proprio perché non si avverte il rischio concreto di procedere con un trattamento non conforme alla normativa vigente e di essere pertanto oggetto di provvedimenti sanzionatori da parte del Garante.

Anche nel caso in cui almeno dal punto di vista formale si è adempiuto a tutti gli obblighi previsti, in realtà spesso non si coglie il vero spirito che ha portato alla promulgazione di questo codice, ovvero la "cultura" del trattamento di dati che si estrinseca nella proattività negli interventi, finalizzata ad evitare danni maggiori, più difficili da risolvere *ex post*. Nella società attuale, fortemente influenzata dalla tecnologia e nella quale la corsa verso nuovi servizi e nuove forme di comunicazione è un obiettivo di molti, risulta sempre più arduo controllare i flussi informativi che transitano ormai da un estremo all'altro del pianeta: da qui l'indiscutibile necessità di garantire ad ogni individuo la possibilità di controllare i propri dati, nel senso di regolarne direttamente le modalità di raccolta e di circolazione, ovvero di interromperne il trattamento nel caso lo si ritenga opportuno ("*diritto d'uscita*").

In conclusione, affinché le disposizioni normative in materia di *privacy* non si riducano ad un semplice adempimento formale, palesemente sterile, è necessario che la protezione dei dati personali venga sentita come un valore a sé stante, solido ma allo stesso tempo fragile qualora non trovi attuazione per mancanza di sensibilità, oppure non venga difeso dagli attacchi provenienti dai sostenitori di diritti in apparenza contrastanti, come ad esempio la sicurezza sociale.

Che significa il principio di “necessità nel trattamento dei dati”?

Il D.Lgs. 196/2003 prevede che i sistemi informativi e i programmi informatici debbano essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento qualora le finalità perseguite nei singoli casi possano essere realizzate, rispettivamente, mediante dati anonimi, ovvero che non riguardino interessati identificati o identificabili, oppure dati non identificativi, ovvero che permettano di identificare l'interessato in maniera indiretta e comunque solo in caso di necessità.

In pratica viene stabilito che i dati personali sono beni preziosi e ad alto rischio, da maneggiare con cura e solo quando ve ne sia effettiva necessità: ad esempio per finalità di ricerche statistiche, non essendo indispensabile conoscere il nome ed il cognome dell'interessato, si dovrà fare a meno di tali informazioni. Questo fondamentale principio viene poi ripreso nell'indicare le modalità del trattamento dei dati e i requisiti degli stessi: infatti è previsto che i dati personali vadano trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o trattati. Si può dunque osservare che questo principio, introdotto con il D.Lgs. 196/03, è in realtà un ampliamento dei principi di *pertinenza e non eccedenza* già previsti della legge 675/96.

Un esempio molto attuale che ben raccoglie tutte le sfumature e le implicazioni del principio di necessità, e dunque di proporzionalità e di finalità, è quello relativo ai sistemi di video-sorveglianza la cui installazione è legittimamente prevista solamente laddove sussistano delle particolari esigenze tali da rendere questa soluzione proporzionata alle finalità perseguite e dove altre misure di sicurezza non risultino sufficienti o praticabili. Ad ogni modo, anche nel caso in cui ci siano tutte le premesse per l'adozione di un sistema di video-sorveglianza, non necessariamente a tutela della protezione di beni, luoghi o persone, il principio di necessità impone che gli strumenti di acquisizione delle immagini siano calibrati in modo tale da non rendere identificabili i soggetti ripresi, qualora tale identificazione non risulti tra le finalità determinate, esplicite, legittime e di pertinenza perseguite (es. video ripresa di luoghi utilizzando telecamere dotate di zoom, e dunque in grado di consentire, almeno potenzialmente, l'identificazione dei soggetti ripresi, per finalità di marketing e promozione turistica).

Analogamente l'impiego di soluzioni biometriche risulta spesso eccessivo e non giustificato alla luce dei principi di necessità e proporzionalità; inoltre, data l'invasività nella sfera personale dell'individuo, tali soluzioni sono da considerarsi come una *extrema ratio* per perseguire finalità di identificazione e controllo, seppur legittime. Ad esempio, l'Autorità Garante ha ritenuto eccessivo, per la finalità perseguita, l'utilizzo della rilevazione delle impronte digitali (piuttosto che del timbro vocale o dell'iride) nel caso di controllo degli

accessi dei dipendenti da parte del datore di lavoro e lo ha conseguentemente vietato in tali contesti.

Si comprende dunque come il principio di necessità porti ad escludere soluzioni tecnologiche altamente invasive della sfera personale, anche qualora queste risultino più economiche o di più semplice applicazione rispetto ad altre, per il cui impiego, nei casi di maggiore invasività, è tra l'altro prevista la preventiva verifica da parte dell'Autorità Garante (*prior checking*).

Anche in contesti particolarmente esposti a minacce, come quelli delle banche, l'Autorità Garante ha ribadito che, per porre in essere misure di sicurezza del tipo appena menzionato, non può difettare il presupposto dell'esistenza di specifiche e concrete esigenze di sicurezza scaturite dalla presenza di particolari rischi.

In conclusione, il principio di necessità assume particolare importanza nella valutazione delle più idonee modalità di trattamento, al fine di assicurare un equo temperamento tra le istanze della sicurezza ed il rispetto della protezione dei dati personali.

Nel suo “Pillole di Privacy” lei definisce il DPS (Documento Programmatico sulla Sicurezza) un “utilissimo strumento di autoanalisi, la cui utilità va ben oltre il mero obbligo normativo”. Può spiegare meglio?

Nell'articolo “*Obbligo di redazione del Documento Programmatico sulla Sicurezza (DPS)*” ho evidenziato come, dall'analisi attenta del testo di legge, dei suoi allegati e delle disposizioni emanate dall'Autorità Garante, sembrerebbe emergere un obbligo formale di redazione del DPS solo da parte di coloro che trattano dati sensibili e giudiziari con strumenti elettronici. In realtà, un Documento Programmatico sulla Sicurezza ben strutturato ed articolato è senza dubbio, per il titolare di trattamenti di dati personali, un validissimo strumento per valutare il proprio sistema di gestione, i propri processi e le criticità che potrebbero condurre ad una loro deviazione dallo standard. Tra l'altro, la semplice redazione del DPS, pur sollevando il titolare da responsabilità penali, lo rende comunque esposto a profili di responsabilità civile nel momento in cui egli arrechi un danno con i trattamenti di cui è responsabile: dunque, al di là degli obblighi formali, è importante redigere un documento che non si limiti a considerare soltanto le contromisure minime di sicurezza per contrastare possibili minacce ai trattamenti, bensì vada oltre e prenda in esame tutte le misure di sicurezza idonee a garantire che, ragionevolmente, i fattori di rischio siano tenuti sotto controllo.

Questo aspetto viene meglio affrontato e chiarito nel volume di prossima pubblicazione da parte dell'Ordine degli Ingegneri della Provincia di Roma, “*Linee guida per la redazione del Documento Programmatico sulla Sicurezza*”, che mi vede autore insieme ai colleghi ingegneri Gianluca Di Tomassi, Alessandro Masci e Christiam Salvatori. Qui si afferma

sostanzialmente che il rispetto della normativa ha come intrinseca finalità quella di indurre un miglioramento dell'organizzazione e della gestione aziendale, in particolare dei processi e degli standard di lavoro, ma anche della qualità e della rispondenza dei risultati ai requisiti prestabiliti.

Più specificamente la redazione del DPS si configura come un valido ausilio all'individuazione delle fonti di rischio, alla loro classificazione in base alla gravità dell'impatto che possono produrre, alla pianificazione temporale delle priorità di intervento per l'abbattimento, o quanto meno per il controllo, dei fattori di rischio ritenuti maggiormente nocivi in relazione alle attività svolte.

Nell'attuale società dell'informazione la capacità di gestire contenuti e dati in modo sicuro, affidabile ed efficiente è sempre più importante per la continuità del lavoro (*business continuity*) e la gestione delle emergenze (*disaster recovery*), ovvero per il mantenimento dei livelli qualitativi prefissati, ed è pertanto questa capacità che distingue fra loro le aziende di successo da quelle che, non riuscendo ad adeguarsi alle continue evoluzioni imposte dal mercato, non sono in grado di affermarsi nel loro settore di competenza.

Da ciò si comprende meglio come la corretta applicazione delle misure (minime) di sicurezza, ovvero di soluzioni tecnologiche specificamente progettate per la tutela della privacy (*privacy enhancing technologies*), consenta non solo di adempiere agli obblighi ed alle formalità di legge, ma soprattutto di migliorare l'organizzazione e la gestione aziendale, ottimizzando e controllando i processi di lavoro in aggiunta alla ragionevole certezza e consapevolezza di operare sempre con dati esatti, corretti, leciti, legittimi, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti, oltre che integri, disponibili ed aggiornati.

Con questa visione e cultura, la stessa organizzazione avrà quindi la garanzia di operare in sicurezza ed in ottemperanza agli adempimenti previsti dal contesto normativo vigente, trasmettendo agli *stakeholder* (clienti, fornitori, creditori, azionisti, etc.) fiducia nei propri riguardi, con un *feed-back* senz'altro positivo per la propria attività.

Quanto appena affermato si integra perfettamente in un sistema di gestione più ampio, che abbraccia anche la qualità (SGQ), ma che va oltre là dove è necessario valutare gli aspetti e gli impatti di una gestione extra-processuale.

In tale contesto diviene chiaro che una gestione sicura, affidabile ed efficiente non vada semplicemente intesa come prevenzione della perdita accidentale di dati aziendali, o assicurazione contro eventuali danni, o ancora più semplicemente un modo per evitare le sanzioni previste in caso di inadempienza, bensì soprattutto come vantaggio competitivo tramite l'adozione di procedure di gestione delle informazioni che permettano di superare tutte le eventuali criticità che potrebbero sorgere da un mancanza di controllo dei processi:

così facendo si trasforma la sicurezza da un costo passivo in un investimento lungimirante e dunque in un vantaggio competitivo.

Di analogo parere è anche il Presidente uscente dell'Autorità Garante, prof. Stefano Rodotà, quando afferma che *“la privacy rappresenta una risorsa che, se intelligentemente impiegata, può rendere più efficiente l'attività d'impresa”*.

Lei lavora presso la Pubblica Amministrazione, dove si occupa di verificare lo stato di adempimento al “Codice in materia di protezione dei dati personali”, in particolare dal punto di vista della sicurezza informatica dei trattamenti elettronici. A che punto è l'adozione di questa normativa nella P.A.? Davvero si ha bisogno ancora una volta di un rinvio del termine per adottare le misure minime di sicurezza?

Mi rammarica molto affermarlo, ma purtroppo le carenze più rilevanti all'interno delle Amministrazioni Pubbliche sono di tipo organizzativo e spesso le inadempienze nascono dalla mancanza di sensibilità e “cultura” verso la protezione dei dati personali, a cui si aggiunge un contatto superficiale con la materia, che svilisce i principi basilari del codice *privacy*, quale ad esempio quello di necessità.

Non si può negare che negli ultimi anni la consapevolezza di queste tematiche sia significativamente aumentata, tuttavia persistono ancora, in taluni contesti, una mentalità ed un approccio di tipo burocratico che non fanno corrispondere ai meri atti formali, pur necessari, una piena coscienza della delicatezza della materia trattata.

D'altra parte è innegabile che i casi di “disattenzione” ministeriale hanno indotto l'Autorità Garante a rinviare già per ben tre volte, se non addirittura quattro, l'obbligo di adozione delle misure minime di sicurezza, prendendo dunque atto che nel settore pubblico risulta di gran lunga più difficile andare oltre la formalità degli adempimenti e pervenire ad un'applicazione sostanziale del codice. A questo proposito, ad esempio, si rileva come alcune Amministrazioni Pubbliche hanno formalmente redatto il Documento Programmatico sulla Sicurezza *una tantum*, vigente la L. 675/96, senza poi far seguito in modo significativo a tale adempimento, anche a causa delle continue proroghe relative al D.Lgs. 196/03: questo atteggiamento di scarsa sensibilità da parte della P.A. non è stato poi in alcun modo migliorato dalle scelte legislative che, anzi, lo hanno accentuato sempre di più ed hanno, inoltre, distolto l'attenzione dalla *privacy* portandola verso altre tematiche ritenute di più stringente attualità.

Un altro effetto di questa situazione nell'ambito pubblico riguarda l'emanazione dei Regolamenti interni sul trattamento dei dati sensibili da parte degli enti pubblici, il cui termine ultimo di presentazione, previsto per la fine del 2005, verrà probabilmente fatto slittare *last minute* anch'esso di un paio di mesi, a causa della mancata predisposizione di

tale documento da parte di molte Amministrazioni. E questo nonostante gli sforzi del Garante di semplificare la produzione dei Regolamenti - adempimento tra l'altro già previsto dalla legge 675/96 - mediante l'emanazione di schemi tipo e la particolare attenzione prestata ai contenuti delle schede che identificano la tipologia di dati sensibili trattati e le operazioni eseguibili in relazione alle finalità perseguite. Anche in questo caso non è piacevole constatare che, nonostante l'Amministrazione in cui opero sia all'avanguardia in materia di *privacy*, avendo addirittura al suo interno un ufficio specializzato e competente, tuttavia non ha ancora ottemperato pienamente a tale adempimento, proprio per problemi di gestione e organizzazione di un dipartimento.

Ancora, un aspetto di particolare delicatezza riguarda il *trade-off* (bilanciamento) tra la trasparenza dell'attività amministrativa - regolata principalmente dalla legge 241/90 sul procedimento amministrativo, così come recentemente modificata dalla legge 15/05 - e la tutela della riservatezza dei dati personali: essendo demandata all'amministrazione destinataria delle richieste di accesso ai dati la facoltà di valutare le motivazioni del richiedente e gli eventuali casi di denegato accesso, il pericolo maggiore è che si possa essere più propensi a negare che a concedere, onde evitare il rischio di provvedimenti sanzionatori. Consapevole di tutto ciò, l'Autorità Garante ha altresì collaborato alla predisposizione di una direttiva del Dipartimento della funzione pubblica, finalizzata a richiamare l'attenzione delle amministrazioni sulle prescrizioni del Codice che incidono maggiormente sulla loro attività e che richiedono per questo l'adozione di efficaci scelte organizzative, al fine di rendere sostanziali le garanzie previste dal legislatore e dunque anche le conseguenze connesse alla loro mancata attuazione.

Infine si accenna brevemente anche al fatto che in alcune realtà accade non di rado che, ai cittadini richiedenti un servizio, non venga fornita l'informativa sul trattamento dei dati personali e che non venga consultata l'Autorità Garante in occasione del varo di norme regolamentari e di atti amministrativi suscettibili di incidere sulle materie disciplinate dal Codice stesso.

Dal contesto delineato risulta evidente che, anche nel settore pubblico, una gestione sicura, affidabile ed attenta alle tematiche presenti nel D.Lgs. 196/03 non è affatto semplice da attuare, anche a causa delle forti resistenze provenienti, non di rado, dall'interno. Dalla mia esperienza in tale settore mi sento di affermare che la volontà dei singoli al miglioramento continuo è presente ed è salda; tale slancio viene, tuttavia, enormemente frenato da un sistema che non vuol rinunciare alle sue certezze e che non sempre è disposto al confronto costruttivo, finalizzato a prendere atto dei suoi punti di debolezza in vista di un loro successivo superamento.

Lei è stato relatore alla “Conference on Network and Information Security: Political and Technical Challenges”, organizzata dall'ISCOM (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione), ove ha trattato la tematica della sicurezza del VoIP con l'intervento “The Voice over Internet Protocol (VoIP) last challenge: Security and Data Protection”. Di che si tratta? Quali sono i rischi nell'utilizzare il VoIP?

L'ISCOM ha organizzato la “Conference on Network and Information Security: Political and Technical Challenges” con l'intento di rinnovare l'attenzione sulle tematiche di sicurezza, oggi spesso trascurate per la corsa a tecnologie sempre nuove ed a servizi sempre più innovativi. Questo evento mi ha visto relatore sulla tematica della sicurezza della tecnologia VoIP, in qualità di Security Consultant della TransTec Services, insieme all'Ing. Christiam Salvatori, partner della società.

Il lavoro svolto ha evidenziato gli aspetti critici delle soluzioni basate sul VoIP (Voice over IP) e che vanno a bilanciare gli indubbi vantaggi che tali soluzioni comportano, quali ad esempio il minore TCO (*Total Cost of Ownership*) rispetto ai sistemi di telefonia tradizionali e la convergenza con le reti dati basate sul protocollo IP.

In particolare, al di là dei rischi per la sicurezza comuni a tutte le reti IP, come virus e worms, sono emerse alcune minacce per la riservatezza, l'integrità e la disponibilità delle comunicazioni strettamente legate alla tecnologia VoIP, o comunque di più semplice attuazione in tale ambito: di seguito se ne riportano alcuni esempi.

Nell'ottica di tutelare la riservatezza delle comunicazioni bisognerà prestare attenzione agli attacchi di *sniffing*, che permettono di intercettare il contenuto delle conversazioni con estrema semplicità se non si adottano adeguate contromisure, come la cifratura della voce trasmessa; un altro tipo di attacco possibile riguarda la capacità di originare chiamate con un identificativo per così dire preso in prestito, al fine di presentarsi al destinatario della chiamata con una identità per lui fidata e sottrargli così informazioni riservate (*phishing*).

Relativamente all'integrità delle comunicazioni, tra le tipologie di attacchi che possono essere condotti si annoverano il *Man-In-The-Middle* o l'alterazione della timbrica vocale, sempre con l'intento di assumere un'identità fidata per l'altra parte della conversazione.

Infine la disponibilità delle comunicazioni può essere compromessa da attacchi di tipo DoS (*Denial of Service*) o SPAM, che con estrema semplicità possono ridurre la Qualità del Servizio offerto in maniera tale da non rendere più intelligibili le chiamate.

D'altro canto non si possono escludere le problematiche intrinsecamente connesse alla tecnologia VoIP, quali l'impossibilità di utilizzarla in assenza di alimentazione elettrica oppure di geo-localizzare la chiamata; quest'ultimo aspetto di geo-localizzazione degli individui nel momento in cui comunicano è un tema di attuale interesse per l'Autorità

Garante, il cui errato utilizzo viene considerato di particolare invasività nella sfera privata degli individui e dunque soggetto a particolari tutele.

La criticità che più di ogni altra emerge da questo scenario è l'impossibilità di garantire il corretto instradamento delle chiamate di emergenza o di soccorso ogni qual volta se ne presenti la necessità, con la conseguenza di limitare molto l'affermazione del VoIP come sostituto della telefonia tradizionale a commutazione di circuito.

Nella conclusione della presentazione è stato poi affrontato lo stato dell'arte della tecnologia VoIP dal punto di vista della sicurezza delle soluzioni commercialmente disponibili e delle prossime sfide volte a rendere ancora più sicure tali soluzioni.

I contenuti trattati in questa risposta saranno comunque ripresi con maggiore esaustività in un White Paper di prossimo rilascio da parte della TransTec Services.

Cos'è la TransTec Services?

La [TransTec Services S.r.l.](#) è una società che fornisce soluzioni nel campo ICT utilizzando le cosiddette metodologie internazionali di "Best Practices". In particolare offre servizi e consulenza nelle seguenti aree: sicurezza di reti ed informatica, protezione dei dati e *privacy* (D.Lgs. 196/03), innovazione e trasformazione tecnologica, sistemi informativi (di gestione, OSS e BSS).

TransTec mette a disposizione un team di professionisti che ha maturato una pluriennale esperienza a livello internazionale. Per far fronte ad un mercato globale altamente concorrenziale, TransTec riconosce nell'innovazione tecnologica, di cui si fa promotrice, lo strumento più efficace per mantenere le aziende competitive. Non a caso l'intervento tenuto da TransTec alla conferenza organizzata dall'ISCOM sul tema "*Network and Information Security: Political and Technical Challenges*" ha mirato ad evidenziare un aspetto che fino a qualche mese fa era trascurato dagli utilizzatori, sempre più in crescita, di questo nuovo mezzo di comunicazione.

Mi allega anche un breve profilo professionale?

Francesco Amendola, laureato con lode in Ingegneria Elettronica - indirizzo Telecomunicazioni, ha conseguito diversi Master in materie tecnico-gestionali ed è iscritto all'Ordine degli Ingegneri della Provincia di Roma, ove è membro della Commissione Informatica e Telecomunicazioni.

Ricopre attualmente la carica di funzionario addetto alla sicurezza ICT presso la Pubblica Amministrazione: si occupa in particolare di rilevazione, monitoraggio, analisi e verifica dello stato della sicurezza informatica e della protezione dei dati personali (D.Lgs. 196/03) all'interno di uffici locali.

$$\Delta x \Delta p_x \geq \frac{\hbar}{2}$$

www.ingamendola.com

Ha inoltre frequentato vari corsi di perfezionamento e specializzazione in materia di sicurezza delle informazioni, tutela dei dati personali e sistemi di gestione presso il CNIPA e presso l'Ordine degli Ingegneri della Provincia di Roma.

Si segnala, tra le esperienze di maggior rilievo, l'attività di relatore in convegni sulla sicurezza delle informazioni e quella di consulenza prestata presso uno dei maggiori *player* del mercato delle telecomunicazioni mobili di terza generazione (H3G S.p.a.).

Ulteriori informazioni sull'autore sono disponibili su www.ingamendola.com

Un particolare ringraziamento è indirizzato alla dott.ssa Antonia Ronzio per la consulenza giuridica offerta

Ing. Francesco Amendola

www.ingamendola.com