Mobile e Privacy

Adempimenti formali e misure di sicurezza per la compliance dei trattamenti di dati personali in ambito aziendale

PRIVACY
On Cloud & Mobile

LICENZA D'USO

Il testo completo della Licenza d'uso è disponibile sul sito di Creative Commons, al link http://creativecommons.org/licenses/by-sa/3.0/it/deed.it

Preghiamo inoltre chi volesse utilizzare questo testo all'interno di propri lavori (non semplicemente con una citazione) di segnalarlo con un messaggio all'indirizzo privacycloudmobile@clusit.it

Indice

Prefazione

Questo documento è frutto del lavoro collettivo di un gruppo di aziende, studi legali e associazioni unite dal comune interesse verso i temi di attualità dell'Information Security. Tale gruppo ha la consapevolezza che, per portare del vero valore aggiunto ai clienti ed in generale a tutti i soggetti interessati, bisogna essere capaci di affrontare i nuovi contesti di business e le nuove sfide che le innovazioni tecnologiche presentano con un **approccio multidisciplinare e omnicomprensivo.**

La Community for Security dispone di tutte le competenze necessarie (di sicurezza, di audit, legali, metodologiche, tecnologiche, ...) per abilitare un significativo confronto interno, avente il fine di produrre dei risultati d'interesse. La Community ha dimostrato il valore di quest' approccio già negli anni scorsi, avendo:

- analizzato e prodotto della documentazione di approfondimento intorno a temi d'interesse, quali "*Gli amministratori di sistema*", "*Il fascicolo sanitario elettronico*"[1] e "*Il ritorno sull'investimento in sicurezza*[2]";
- portato il proprio contributo ad una serie di convegni e conferenze (proprie e di terzi).

Quest'anno la Community ha deciso di cimentarsi contemporaneamente con due gruppi di lavoro distinti, sui temi della ***Mobile e Privacy*** e della ***Privacy nel Cloud***. Questo documento raccoglie le risultanze e gli spunti emersi dalle analisi correlate al primo argomento.
L'approccio scelto è verticale: il Gruppo di Lavoro si è infatti concentrato sulle specifiche sfide che l'adozione in ambito aziendale di dispositivi mobili evoluti (generalmente identificati come *smartphone* e *tablet*) comporta rispetto **alla corretta gestione ed alla protezione dei dati personali trattati, per i quali l'azienda risulti titolare ai sensi del D.Lgs.196/03 (Codice Privacy)**.

In particolare, le analisi, pur basandosi su una significativa bibliografia sulla tematica, sono state realizzate cercando di ridurre al minimo ripetizioni di informazioni già presenti in altri studi nazionali ed internazionali sul *Mobile* e focalizzandosi, invece, sullo **specifico ambito normativo Privacy italiano.**
In tal senso, il documento presenta in maniera sintetica, quali elementi normativi e di sicurezza tenere in considerazione nel momento in cui si realizzino trattamenti di dati personali mediante tali dispositivi e di come indirizzare quegli aspetti di protezione di natura tecnologica, procedurale ed organizzativa, ivi comprese anche quelle misure che il legislatore non ha esplicitamente richiesto (le c.d. misure idonee).

Riteniamo che tale approccio possa supportare opportunamente tutti coloro che hanno già adottato o che hanno in procinto di adottare tali dispositivi per effettuare trattamenti di dati personali o più in generale per supportare opportunamente i propri processi di business.

[1] Il documento di analisi del provvedimento del Garante della Privacy sul Fascicolo Sanitario Elettronico è liberamente disponibile a questo link http://fse.clusit.it in forma sintetica e per mail in forma completa.
[2] Il documento di analisi relativo ai ritorni sugli investimenti in sicurezza è disponibile a questo link http://rosi.clusit.it/pages/Homepage.html

Executive Summary

La vorticosa innovazione tecnologica di questo inizio secolo ha permesso l'affermazione, in ambito aziendale, di nuovi modelli di business. Fenomeni quali la diffusione dei social network e delle soluzioni di cloud computing, se opportunamente sfruttati, sono in grado di rivoluzionare i paradigmi operativi, offrendo enormi potenzialità.
Uno di tali fenomeni, affermatosi negli ultimi anni, è sicuramente quello legato all'adozione, per finalità di business, dei cosiddetti dispositivi mobili evoluti, volendosi riferire con tale accezione ad apparecchi quali *tablet*, *Smartphone* o più in generale a qualsiasi strumento, connesso a reti telefoniche e/o telematiche in grado di offrire una significativa capacità elaborativa, nonostante un limitato ingombro fisico. Pur non essendo, di per sé, un elemento nuovo, in quanto derivato dalla convergenza di utilizzo dei telefoni mobili e dei computer portatili (*laptop* prima e *netbook* poi) verso una maggiore ibridizzazione, esso sta avendo particolare rilevanza sia per effetti di "moda" (l'adozione degli *smartphone* è avvenuta in prevalenza prima in ambito *consumer* e poi in ambito professionale, fenomeno denominato *consumerization*), sia per le caratteristiche peculiari di tali dispositivi, che promettono dei potenziali vantaggi competitivi e benefici non irrilevanti. Tali vantaggi, esaltati dalla contemporanea affermazione di ulteriori trend tecnologici (l'aumento della disponibilità e delle prestazioni delle connessioni dati ed i già citati servizi di cloud computing), sono correlabili alla possibilità di poter raggiungere, consultare ed elaborare dati ed informazioni in qualsiasi momento e luogo.

Ovviamente però, oltre agli indiscutibili benefici, l'adozione di tali dispositivi introduce specifici elementi di rischio (nuovi o già esistenti). Mentre alcuni di essi sono particolarmente evidenti e citati in qualsiasi studio (furto o smarrimento degli strumenti), altri sono spesso oggetto di minor attenzione, aspetto di particolare criticità, dato che la mancata o la parziale analisi di possibili fonti di minacce può determinare delle potenziali vulnerabilità per i dati e le informazioni a disposizione in ambito aziendale, rappresentanti uno dei principali (se non il principale) asset aziendali. E tra le diverse tipologie di dati ed informazioni esistenti spiccano, per pervasività e per complessità della normativa cogente, i dati personali.

L'obiettivo del presente documento è pertanto quello di evidenziare rischi, adempimenti formali e misure di protezione da tenere in considerazione nel trattamento di dati personali mediante tali dispositivi. Dato che la tematica può essere affrontata secondo diversi prospettive, il documento indirizza
i rischi e gli aspetti legali, procedurali, organizzativi e tecnologici che una società titolare di trattamenti di dati personali in ambito italiano effettuati mediante smartphone e tablet, deve prendere in considerazione affinché tali trattamenti siano svolti nella conformità alla normativa applicabile e garantendo un opportuno livello di sicurezza.

Sono dunque esclusi dall'analisi del presente documento elementi quali i trattamenti di dati personali fatti su dispositivi in possesso di utenti di servizi mobili o i trattamenti fatti sui dati generati dai dispositivi da parte di società di servizi di telecomunicazione.

Data l'ampiezza dell'ambito, le analisi effettuate dal Gruppo di Lavoro hanno dedicato una particolare attenzione ai requisiti ed agli adempimenti indicati dalla normativa Privacy italiana, focalizzandosi però non solo sui requisiti cosiddetti "minimi ed obbligatori", ma prendendo in considerazione quegli elementi di sicurezza indicati quali "misure idonee".

Tali analisi hanno permesso al Gruppo di Lavoro di determinare le seguenti osservazioni, poi riprese in maniera più dettagliata nello sviluppo del documento:

- l'introduzione dei dispositivi mobili evoluti (quali tablet e smartphone) in ambito aziendale deve essere effettuata solamente a fronte di un'attenta e strutturata analisi dei rischi, che tenga conto delle specifiche aree critiche correlabili all'ambito dei trattamenti di dati personali effettuati, indirizzando, di conseguenza, le misure di sicurezza e di compliance normativa correlate;

- le aree critiche sono principalmente correlabili ad aspetti di natura tecnologica (eterogeneità delle caratteristiche tecnologiche di questi dispositivi, complessità del portafoglio degli asset, esistenza di vulnerabilità tecniche…), ma anche ad elementi quali: comportamenti non idonei da parte delle risorse umane, mancato rispetto degli adempimenti formali nel loro utilizzo;
- la mancanza di conformità normativa in merito agli adempimenti formali della normativa Privacy cogente (informative, consensi, notificazioni…) rappresenta una delle principali criticità. È possibile che i trattamenti effettuati con strumenti appartenenti all'ambito mobile possano essere non conformi rispetto al Codice Privacy e/o a provvedimenti dell'Autorità Garante per la Privacy, malgrado l'azienda sia dotata delle necessarie ed opportune misure di sicurezza. Attività di trattamento di dati personali particolarmente critici, quali, ad esempio, quelli legati alla geolocalizzazione dei dispositivi possono essere realizzate solamente a fronte di un opportuno preventivo indirizzamento degli aspetti legali (notificazione, informative…);
- per garantire una piena conformità alla normativa, è altresì necessario che siano adottate soluzioni che soddisfino sia le cosiddette misure minime, contenute nel disciplinare tecnico (Allegato B del Codice Privacy) sia quelle obbligatorie (indicate nei provvedimenti specifici dell'Autorità Garante Privacy). Le misure minime specificate dall'attuale normativa, sono state però definite per un contesto tecnologico generale, che non tiene conto di alcuni elementi peculiari dei dispositivi mobili evoluti. Pertanto, pur essendo le stesse valide universalmente, si ritiene possa essere necessario un loro ripensamento, per la loro implementazione nel contesto di utilizzo dei dispositivi mobili evoluti. Le prescrizioni relative agli aspetti di sicurezza quali il controllo degli accessi logici, il salvataggio dei dati e l'adozione di soluzioni anti-malware per essere completamente soddisfatte nell'ambito mobile, devono essere opportunamente ri-analizzate alla luce delle caratteristiche dei dispositivi;
- un'indicazione analoga è altresì ipotizzabile anche per le misure ritenute obbligatorie introdotte da specifici provvedimenti. Provvedimenti, quali quello degli amministratori di sistema (provv. Autorità Garante Privacy del 27.11.2008 e successive modifiche e integrazioni) e o della dismissione RAEE (provv. Autorità Garante Privacy del 13.10.2008) possono essere pienamente soddisfatti, solo se si considerano opportunamente le peculiarità dei dispositivi. Ad esempio, ai sensi di quest'ultimo provvedimento, la dismissione dei dispositivi deve prevedere una corretta cancellazione dei dati presenti in tutti gli elementi del dispositivo (memoria interna, sim, scheda di memoria esterna…);
- relativamente, infine, alle cosiddette misure idonee di sicurezza, si evidenzia che esse dovrebbero derivare dalla succitata analisi dei rischi, correlata allo specifico ambito operativo. Tuttavia, a prescindere da tale specifico ambito, il Gruppo di Lavoro ritiene che alcune misure debbano essere considerate, nel contesto tecnologico e di business attuale, quali imprescindibili ai fini di una corretta protezione dei dati personali trattati.

Ragioni, obiettivi e ambito del documento

Ragioni

Nonostante non possa essere ritenuta fortemente innovativa[3], la tematica dei trattamenti di dati ed informazioni attraverso dispositivi portatili ha subìto nell'ultimo periodo un notevole aumento di attenzione da parte di varie tipologie di soggetti (imprese, esperti del settore della sicurezza, autorità competenti e perfino singoli utenti di tali dispositivi).
Tale nuova ondata di interesse è stata principalmente determinata dall'aumento vertiginoso di adozione di dispositivi mobili evoluti (smartphone e tablet[4]), in primis in ambito privato e successivamente anche in ambito lavorativo, tanto da fare ipotizzare ad alcuni analisti del settore, che essi possano soppiantare i precedenti dispositivi portatili in orizzonti temporali ben più brevi di quelli inizialmente attesi.

L'affermazione di queste tipologie di dispositivi è caratterizzata da una serie di elementi di natura tecnologica, normativa e sociologica che delineano dei contesti operativi aziendali significativamente innovativi, opportunamente evidenziati nei capitoli seguenti, che rendono particolarmente interessante la ridefinizione degli approcci adottati per i trattamenti di dati personali. Tra tali elementi quelli maggiormente rilevanti e funzionali al presente studio, ovvero:

- **I ruoli e le dinamiche dei player del settore:** i ruoli dei soggetti del settore (produttori di dispositivi, di sistemi operativi, di piattaforme, produttori e commercializzatori di application…) sono sempre più labili ed in continua evoluzione. Tale situazione determina una notevole difficoltà nell'identificazione di soluzioni tecnologiche di player stabili e/o standardizzate, facilitando quindi una coesistenza di vari fornitori tecnologici in continua evoluzione.
- **L'eterogeneità e la numerosità dei dispositivi:** in accordo con quanto detto al punto precedente, e in relazione alla soddisfazione di specifiche esigenze dei vari soggetti utilizzatori, il mercato offre una moltitudine estesa di soluzioni tecnologiche che, seppur muovendosi all'interno di specifici ambiti tecnologici (i.e. mondo Apple vs mondo Android vs RIM…), sono caratterizzate da combinazioni dispositivo-Sistema Operativo-operatore TLC-application vendor, tali da rendere il parco tecnologico particolarmente eterogeneo e quindi di difficile governo. Senza contare le numerose funzionalità tecnologiche che possono caratterizzare ognuno di tali dispositivi in termini ad esempio di connettività, disponibilità di funzionalità di georeferenziazione, dimensioni memoria, ecc.
- **L'utilizzo ibrido dei dispositivi in ambito aziendale:** le principali finalità per le quali le imprese hanno deciso di adottare tali dispositivi sono molteplici e correlate sia alle attività core-business[5] che altresì alle attività di supporto dello stesso[6]. A prescindere da tali specifiche attività, ciò che comunque caratterizza l'adozione in azienda è però l'uso fortemente promiscuo (lavorativo-personale) che si sta affermando, che determina una particolare complessità nella gestione di tutti gli aspetti correlati e della protezione dei dati personali (riferibili sia ai clienti dell'azienda che ai dipendenti).
- **I nuovi approcci gestionali relativi alla tematica:** in relazione anche ai punti precedenti, si stanno affermando approcci alla gestione dei dispositivi mobili che determinano delle vere e proprie rivoluzioni nel concetto di gestione e protezione dei dati e delle informazioni. In particolare sempre più società stanno prendendo in considerazione quello che viene identificato come approccio/ politica di BYOD (Bring Your Own Device), ovvero la scelta di permettere ai propri dipendenti di utilizzare i dispositivi mobili che preferiscono, spostando quindi la linea di protezione dei dati alle fonti degli stessi (database, archivi destrutturati, cartelle di rete…).

[3] Basti pensare alla ormai ventennale ampia diffusione di dispositivi portatili, quali notebook, netbook, dispositivi di memoria ottici e non, cellulari…

[4] Con tali accezioni si vogliono qui di seguito ricomprendere anche tutti quei dispositivi analoghi, quali palmari, la cui categorizzazione non è di immediata realizzazione dato il forte livello di ibridizzazione che sta caratterizzando i dispositivi portatili (in tal senso basti pensare che un netbook con una qualsiasi connessione, mobile o wireless, dotato di software quali Skype può garantire funzionalità simili ad uno smartphone, ovviamente con le opportune caratteristiche differenziali).

[5] Ad esempio per garantire un'assistenza continuativa a clienti, per ottimizzare servizi logistici, per accedere da remoto a servizi on-line…

[6] Ad esempio per l'erogazione di servizi di e-learning, per dare accesso a informazioni aziendali delle funzioni di staff…

- **I rischi correlati e la loro attuale percezione:** la massiccia adozione di questi dispositivi, con le loro caratteristiche tecnologiche ed i risvolti sociologici nell'utilizzo, richiederebbe una riconsiderazione dei rischi correlati. Ciononostante, diversi studi sulla tematica hanno evidenziato che gli utenti, focalizzano la loro attenzione su rischi già esistenti e facilmente percepibili (quale ad esempio lo smarrimento o il furto del dispositivo) e considerano meno altri (quali ad esempio gli accessi non autorizzati o l'infezione da codice malevolo), senza effettivi razionali alla base di tale percezione.
- **Il contesto normativo e gli standard di sicurezza:** il contesto normativo attuale e gli standard di sicurezza sono ancora in buona parte fortemente orientati ad indirizzare aspetti dei trattamenti effettuati mediante dispositivi fissi o portatili (ovvero nei contesti tradizionali).

Obiettivi

Partendo da tali presupposti e relativamente alla sicurezza ed alla *compliance* dei dati e delle informazioni nei dispositivi mobili, sono già molto numerosi gli studi che si sono dedicati ad analizzare la tematica sotto diversi punti di vista con focus molto specifici o tecnici, altri limitandosi ad evidenziare gli elementi principali legati a questa innovazione tecnologica.
Allo stesso tempo, l'Autorità Garante per la Privacy, attraverso la pubblicazione della brochure di comunicazione "*Smartphone e tablet: scenari attuali e prospettive operative*" ha altresì riportato l'attenzione sulla protezione dei dati personali dei possessori di tali dispositivi, evidenziandone rischi ed aspetti critici.

L'obiettivo che il gruppo di lavoro si è prefissato nella predisposizione del presente documento vuole essere quello di trait d'union tra questi due approcci, evidenziando gli aspetti di rischio introdotti dall'utilizzo di tali dispositivi e le misure che possono essere adottate per gestirli, in un contesto specifico: quello aziendale.
Pertanto, il principale scopo è quello di fornire un compendio degli aspetti di natura legale, organizzativa, procedurale e tecnologica che devono essere considerati e gestiti in ambito aziendale qualora vengano effettuati dei trattamenti di dati personali attraverso dispositivi mobili evoluti (secondo l'accezione meglio specificata nel paragrafo successivo), al fine di garantire la piena conformità alle normative Privacy cogenti.

Ambito

Il punto di partenza è la posizione di titolarità che la società ricopre nel trattamento dei dati personali, con particolare attenzione alle tipologie di soggetti interessati di maggiore interesse, che saranno egualmente trattate nel documento, ovvero:

- i clienti (finali o diretti) della società, i cui dati possono essere trattati per le diverse finalità aziendali (custode care, profilazione, …);
- i dipendenti della società, i cui dati possono essere trattati per motivi operativi, retributivi, disciplinari,…
- gli ulteriori soggetti interessati quali fornitori, partner di business…

Il Gruppo di Lavoro ha scelto tale obiettivo in quanto elemento preponderante sia al fine di evitare di incorrere in trattamenti non conformi all'attuale normativa vigente (e nelle eventuali sanzioni correlate), sia per implementare una gestione degli stessi che possa determinare degli effettivi vantaggi competitivi a prescindere dalla dimensione e dal settore di operatività dell'impresa.

Se infatti la corretta conduzione dei trattamenti dei dati personali in questione è, in primis, un elemento di sicurezza e di compliance normativa, è altresì vero che, laddove correttamente impostati, i trattamenti possono costituire dei veri e propri differenziali competitivi: si pensi ad esempio alla possibilità di garantire un servizio di supporto continuativo attraverso l'accesso ai dati da questi dispositivi o all'ottimizzazione di servizi logistici avvalendosi delle informazioni messe a disposizione dai dispositivi assegnati ai dipendenti.

Terminologia e riferimenti bibliografici

Al fine di trattare opportunamente le tematiche del documento è opportuno che siano definite le seguenti accezioni/i seguenti acronimi peculiari del contesto *mobile*, di seguito evidenziati:

Apps: Applicazioni per dispositivi mobili che si possono essere rese disponibili / scaricate da diverse fonti, quali siti pubblici on-line correlati a piattaforme dei produttori dei dispositivi, siti pubblici on-line non correlati a specifici produttori, elenchi di applicazioni sviluppate in ambito aziendale…
Bluetooth: standard tecnico-industriale di trasmissione dati per reti personali senza fili (WPAN: Wireless Personal Area Network). Fornisce un metodo standard, economico e relativamente sicuro per scambiare informazioni tra dispositivi diversi attraverso una frequenza radio a corto raggio.
BYOD (Bring Your Own Device): approccio per l'utilizzo di dispositivi mobili evoluti in ambito aziendale che prevede che gli utenti dei servizi informativi aziendali possano utilizzare il dispositivo di loro maggiore gradimento.
GPS (Global Positioning System): sistema di posizionamento e navigazione satellitare in grado di rilevare e fornire la posizione di uno specifico dispositivo predisposto per il tracciamento correlato.
ISPA (Information Security Policy Architecture): insieme strutturato di policy per la sicurezza delle informazioni, predisposte in ambito aziendale.
Jailbreaking: attività effettuata su un dispositivo (generalmente contro le regole che ne determinano l'utilizzo), al fine di permettere un'estensione dei servizi IT disponibili.

MAM (Mobile Application Management): sistemi centralizzati per la gestione strutturata delle applicazioni mobili adottate in ambito aziendale.
MDM (Mobile Device Management): sistemi centralizzati per la gestione strutturata dei dispositivi mobili evoluti in ambito aziendale.
NFC (Near Field Communication): tecnologia che fornisce connettività wireless a radiofrequenza bidirezionale a corto raggio (fino ad un massimo di 10 cm), attualmente di forte interesse per sistemi evoluti di pagamento per i dispositivi mobili evoluti.
PCI-DSS (Payment Card Industry – Data Security Standard): Standard di sicurezza delle informazioni per organizzazioni che trattano informazioni degli utilizzatori di carte di credito, debito, prepagate e similari.
RAEE: rifiuti di apparecchiature ed elettroniche.
RID (Riservatezza Integrità e Disponibilità): i tre requisiti principali per la sicurezza dei dati e delle informazioni in ambito aziendale della sicurezza delle informazioni.
Sandboxing: misura di sicurezza che consiste nella limitazione dell'esecuzione delle applicazioni installate sui dispositivi.
SD/MMC (Secure Digital): più diffuso formato di schede di memoria, dispositivi elettronici utilizzati per memorizzare in formato digitale grandi quantità di informazioni all'interno di memorie flash. La MultiMediaCard (MMC) è stato un altro standard di memory card, molto simile.
SIM (Subscriber Identity Module): particolare Smart card denominata UICC, ma nota informalmente come SIM card, che viene usata nei telefono cellulari per identificare il numero dell'abbonato.
Smartphone: uno smartphone è un dispositivo portatile, alimentato a batteria, che coniuga le funzionalità di telefono cellulare con quelle di elaborazione e trasmissione dati tipiche del mondo dei personal computer.
Tablet: i tablet o tablet computer sono dispositivi assimilabili per componenti hardware e software agli smartphone, dai quali si distinguono per dimensioni dello schermo, possibile assenza del modulo telefonico, destinazione d'uso.
VPN (Virtual Private Network): modalità di trasmissione dati in modalità privata (criptata o analogo) su rete pubblica, tipicamente Internet.
Walled Gardens: misura di sicurezza di carattere preventivo che consiste nella limitazione del contesto tecnologico applicabile, con riferimento, per esempio ad una limitazione delle applicazioni installabili sui dispositivi.

WiFi: Standard tecnico-industriale di trasmissione dati che consente a terminali di utenza di collegarsi tra loro attraverso una rete locale in maniera wireless (WLAN) basandosi sulle specifiche dello standard IEEE 802.11.

Tali accezioni e acronimi, unitamente ad alcuni aspetti contenutistici del documento sono basati sulle analisi e sulle riflessioni contenute nel seguente indice bibliografico.

- *Securing consumer devices*, Information Security Forum ISF, Aprile 2011.
- *Managing the Mobile Workforce*, Tech Target, Giugno 2011.
- *A Window Into Mobile Device Security*, Symantec, 2011.
- *Critical Capabilities for Mobile Device Management*, Gartner Group, Luglio 2011.
- *The Current State of Cybercrime and What to Expect in 2012-RSA 2012 Cybercrime Trends report*, RSA, gennaio 2012.
- *Shining the "Spotlight" on Mobile*, SC Magazine, maggio 2011
- *Applicazioni Mobili che caratteristiche avranno e quali saranno quelle di maggior successo*, Executive.it, aprile 2011.
- Geolocation: risk, issues and strategies, ISACA, 2011.
- *Osservatorio Mobile Internet, Content & Apps*, School of Management Politecnico di Milano, 2011.
- *Consumer and Convergence*, KPMG, 2010.
- *"Mobile device security: understanding vulnerabilities and managing risks",* Ernst & Young, 2012.
- *Selecting the right mobile device management solution: On-premise, managed service or SaaS*, Wavelink, luglio 2011
- *Osservatorio New Tablet e Business Appkication,* School of Management Politecnico di Milano, 2011.

Tra i riferimenti di maggiore interesse, una particolare segnalazione riguarda la pubblicazione "*Smartphone e tablet: scenari attuali e prospettive operative*" dell'Autorità Garante per la Protezione dei dati personali, presentata nel mese di giugno 2011 al Parlamento italiano, in occasione della relazione annuale.

Inquadramento generale relativo ai dispositivi mobili evoluti

Premessa

Prima di procedere con l'analisi dettagliata dei benefici e dei rischi della realizzazione di trattamenti di dati personali attraverso dispositivi mobili evoluti, si ritiene opportuno evidenziare il contesto generale correlato.

Con il termine *dispositivi mobili*, si fa generalmente riferimento a quegli strumenti informatici che nonostante una limitata dimensione fisica permettono di usufruire di *feature* elaborative e/o di servizi correlati. Data l'ampiezza di tale definizione, risulta chiaro come possano essere quindi ricompresi anche strumenti non particolarmente innovativi quali notebook, netbook, cellulari anche di non recente generazione, palmari e molte altre tipologie di dispositivi.

Pur non sottovalutando l'importanza di tutte queste apparecchiature, ma volendo bensì evidenziare come una corretta strategia di protezione dei dati e delle informazioni debba tenere conto di tutti i diversi contesti tecnologici presenti in azienda, il Gruppo di Lavoro si è focalizzato su quelli che sono generalmente definiti dispositivi mobili evoluti, intendendo riferirsi con tale accezione principalmente agli smartphone ed ai tablet. Tale scelta è stata determinata sulla base della vorticosa affermazione che tali strumenti stanno avendo in ambito aziendale e dalle enormi potenzialità di business correlate al loro impiego.
Per dare l'idea di tale evoluzione basta analizzare i risultati dell'Osservatorio New Tablet & Business Application del Politecnico di Milano[7] dove interrogati sui trend e le aspettative in termini di dispositivi, quasi il 75 % dei CIO e dei business manager ha evidenziato "*di aver già introdotto in ambito aziendale i Tablet o di aver intenzione di farlo nel futuro*". Quanto agli smartphone, si può tranquillamente affermare come essi siano ormai una realtà radicata nel portafoglio tecnologico delle imprese.

Ma quali elementi, quali funzionalità caratterizzano tali dispositivi? E perché si considera la loro introduzione in ambito aziendale come un elemento di peculiare innovazione piuttosto che una semplice evoluzione incrementale?

Le caratteristiche dei dispositivi mobili evoluti (smartphone e tablet)

Smartphone. Con il termine di *smartphone* si fa generalmente riferimento a dispositivi in grado di offrire servizi di telecomunicazione telefonici / telematici (e quindi generalmente anche di posizionamento GPS), disponendo contemporaneamente di potenza di calcolo, memoria e funzionalità informatiche analoghe a quelle dei computer portatili di limitate prestazioni. Di fatto, tali dispositivi sono dei cellulari con dimensioni compatte, di recente generazione dotati di sistemi operativi, che permettono di supportare *feature* applicative di elevato interesse per l'utente (associabili ad elementi di multimedialità, di connettività o di elaborazione dati).

Ulteriori elementi caratterizzanti, evidenziati nei diversi documenti bibliografici indicati in precedenza sono identificabili in:

- dimensione relativamente contenuta dei display e delle tasterie (pur se QWERTY o virtuali), che rende complicata la realizzazione di alcune tipologie di attività (e.g. gestione di fogli di calcolo…);
- costo contenuto (con forte trend discendente);
- elevata disponibilità di applicativi (di seguito indicati più semplicemente come Apps), generalmente correlati al produttore del dispositivo o alla piattaforma del sistema operativo adottato;
- ulteriori possibilità di connettività (oltre a quelle dell'infrastruttura degli operatori telefonici), quali Wi-Fi, Bluetooth.

[7] Osservatorio dell'ottobre 2011 acquisibile al sito http://www.osservatori.net/hom

Tali caratteristiche, congiuntamente all'*appeal* generato da ulteriori elementi peculiari di alcuni dispositivi quali l'interattività mediante *touch screen*, hanno determinato un'elevata diffusione pressoché totale (ovvero un dispositivo a persona), dapprima nel mondo *consumer* ed in seguito in ambito business (secondo il fenomeno indicato come *Consumerization*).

Tablet. Con il termine *tablet* ci si riferisce, invece, generalmente, a dispositivi di elaborazione dati che dispongono di potenza elaborativa e di funzionalità analoga a computer di medie prestazioni e che a causa di un display di dimensioni maggiori (generalmente sopra i 7") hanno delle dimensioni meno compatte degli smartphone (i.e. non stanno in una mano), pur garantendo una maggiore "comodità" rispetto a notebook. Ulteriori elementi caratterizzanti sono:

- display touchable;
- disponibilità di accessori quali tastiere aggiuntive e stilo per input dati;
- possibilità (ma non per tutti i tablet) del modulo di connettività all'infrastruttura telefonica degli operatori TLC (sempre presente in genere invece quella di connettività telematica).

Tali dispositivi rappresentano il perfetto concetto del trend di *ibridization* dei dispositivi potendo essere considerati, appunto, una soluzione intermedia tra un computer portatile e uno smartphone.
Sempre secondo l'osservatorio del Politecnico, l'elemento innovativo introdotto dai tradizionali device mobili e dagli smartphone sembra essere riconducibile "*alle diverse caratteristiche fondamentali della mobility applicata al Business: elevata portabilità, buona capacità di visualizzazione e potenza di calcolo. I New Tablet, inoltre, si differenziano dagli altri device mobili anche per alcune peculiarità innovative in grado di influenzare la user experience: introducono una modalità di fruizione radicalmente diversa, abilitata dall'utilizzo di schermi multitouch; sono "always on", sempre disponibili e con tempi di accensione pressoché istantanei, grazie alla diffusione delle memorie a stato solido; infine, sono estremamente efficaci per la condivisione dei contenuti multimediali visualizzati con le persone in prossimità/con cui si interagisce*".[8]

Ovviamente le suddette classificazioni presentano sempre più dei confini labili, in quanto:

- le due tipologie di dispositivi condividono elementi tecnologici comuni (il sistema operativo di base, ma anche le eventuali infrastrutture centralizzate di gestione);
- tutti questi dispositivi hanno la capacità di aumentare la memoria, tramite l'utilizzo di schede di memoria (SD o altri formati), in alloggiamenti opportunamente predisposti;
- gli smartphone e i tablet hanno funzionalità molto similari, soprattutto in merito all'acquisizione ed utilizzo delle Apps;

Anche i produttori di dispositivi sembrano spingere il mercato lungo tale direttrice di ibridizzazione: tastiere virtuali e schermi espandibili sono due elementi di prossima possibile evoluzione ed uno strumento in grado di stare in mano/in una tasca, integrabile poi a richiesta con altri dispositivi fisici, da scrivania o virtuali, è infatti l'ambito di sviluppo.

Le principali piattaforme e le dinamiche di settore

Oltre alle specifiche funzionalità che ogni singolo dispositivo può offrire, nell'ottica delle analisi del presente documento è utile, inoltre, evidenziare anche le attuali dinamiche del settore, partendo dall'individuazione delle principali piattaforme (in termini di sistema operativo adottato):

- **iOS:** sistema operativo adottato dai dispositivi della società Apple (iPhone insieme ad iPod, iPad e, con un'interfaccia differente, anche Apple TV di seconda generazione). Conosciuto come iPhone OS, prima dell'aprile 2010 è una versione ottimizzata del sistema operativo Mac OS X (privato delle componenti non necessarie). Le differenze tra il sistema operativo utilizzato dai computer e quello utilizzato dal cellulare non sono note, ma è possibile dire che è basato su una variante dello stesso kernel e include il componente "Core animation" che supporta le animazioni dell'interfaccia.

[8] Ibidem

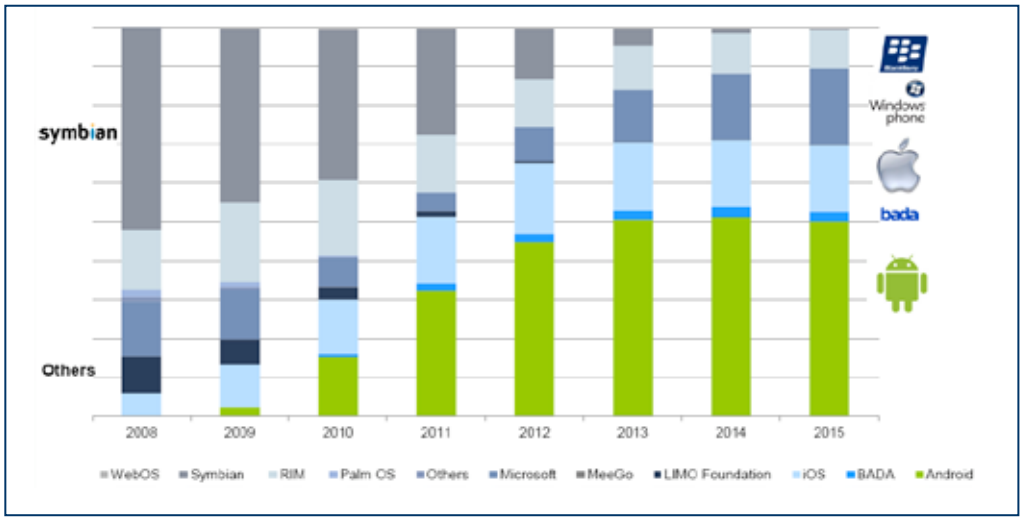
La Springboard è l'interfaccia principale dell'iPhone. È composta dalle icone dei programmi su uno sfondo nero (a scelta dell'utente a partire da iOS 4) e sotto è presente un dock con le applicazioni telefono, e-Mail, Safari e iPod (oggi personalizzabile secondo le priorità dell'utente). Le funzioni del dispositivo sono accessibili mediante un innovativo schermo tattile, chiamato multi-touch, che non necessita di pennino ma si utilizza direttamente con le dita e permette di gestire il tocco di più dita contemporaneamente. Questa caratteristica permette di implementare le cosiddette gesture, ovvero combinazioni di gesti, movimenti di più dita, che permettono di controllare l'interfaccia del dispositivo.

- **Android:** prodotto da un consorzio il cui capofila è Google, è costituito da uno stack software che include un sistema operativo di base, i middleware per le comunicazioni e le applicazioni di base, tale sistema operativo è stato adottato da diverse società produttrici di dispositivi. Ha avuto successo perché alcune versioni sono state open source e perché è basato su kernel Linux. Le applicazioni vengono eseguite tramite la Dalvik virtual machine, una macchina virtuale adattata per l'uso su dispositivi mobili. Android è fornito di una serie di applicazioni preinstallate: un browser, basato su WebKit, una rubrica e un calendario..
- **Symbian:** Il Symbian OS è stato per anni il sistema operativo dei cellulari Nokia. L'ultima versione disponibile del sistema operativo è la 5.0. L'11 febbraio 2011 Nokia ha scelto di adottare sul proprio hardware il nuovo sistema operativo di Microsoft, Windows Phone 7, come "piattaforma principale" affiancando la piattaforma Symbian. Il 27 aprile 2011 Nokia ha annunciato l'esternalizzazione totale dello sviluppo della piattaforma Symbian alla società Accenture, già da tempo partner strategico della società finlandese.
- **Windows Phone:** Windows Phone, precedentemente Windows *Mobile* e ancora prima Pocket PC, è un sistema operativo compatto basato sulle API Win32 di Microsoft. Fra i dispositivi che ne possono essere equipaggiati ci sono i Pocket PC, gli Smartphone ed i Portable Media Center. Alla fine di settembre del 2011 la Microsoft ha rilasciato l'aggiornamento annuale definito Windows Phone 7.5 (o 'Mango'). Il termine "Windows CE" (compact edition) è in realtà il nome "tecnico" con il quale viene indicata la piattaforma generale di sviluppo di questo sistema operativo. Essendo "Windows CE" sufficientemente modulare e flessibile, sono state sviluppate delle specifiche versioni per dispositivi differenti (oltre che per processori differenti dal x86, quali MIPS, ARM e Hitach SuperH). Il sistema prevede versioni ridotte dei classici MS Office e Windows Media Player.
- **BlackBerry:** BlackBerry OS è un sistema operativo *mobile* proprietario, sviluppato da Research In Motion per la sua linea di smartphone BlackBerry. Il sistema operativo fornisce multitasking e supporta dispositivi di input specializzati che sono stati adottati da RIM, in particolare la rotellina (trackball) e più recentemente il trackpad e touchscreen. La piattaforma BlackBerry è forse più nota per il suo supporto nativo della posta elettronica aziendale attraverso MIDP 1.0 (*Mobile* Information Device Profile) e più recentemente, un sottoinsieme di MIDP 2.0, che consente di completare l'attivazione wireless e la sincronizzazione con Microsoft Exchange, Lotus Domino o Novell GroupWise, per la sincronizzazione di e-mail, calendario, attività, note e contatti (necessità l'attivazione del BlackBerry Enterprise Server). A settembre 2010, RIM ha annunciato un nuovo sistema operativo, la piattaforma QNX, BlackBerry Tablet OS, che opererà su BlackBerry PlayBook. QNX andrà a sostituire completamente BlackBerry OS a partire dalla versione 8. La versione 2.0, annunciata il 18 ottobre 2011 da RIM come versione beta, che supporta Adobe Air 3.0 e Adobe Flash 11, così come WebGL. Inoltre viene introdotto anche il BlackBerry OS Runtime per eseguire le applicazioni Android, riconfezionati utilizzando strumenti presentati e pubblicati tramite BlackBerry App World.

Secondo le proiezioni Gartner, tale suddivisione del mercato complessivo avrà le caratteristiche rappresentate nella Figura 1.

Figura 1
Mobile OS Market Shares and Forecast 2008-2015

Fonte: Gartner 2011



Questa breve panoramica permette di evidenziare sommariamente come, anche considerando solo alcuni aspetti dei principali player, siano numerosi i diversi elementi tecnologici (ma non solo), che i responsabili aziendali devono considerare all'atto di scegliere quali dispositivi adottare in azienda. Inoltre, è possibile rilevare come, a prescindere dalle specifiche caratteristiche tecnologiche dei dispositivi, il settore si presenti dal punto di vista dei *player* piuttosto variegato e mutevole, con un continuo susseguirsi di alleanze, partnership, acquisizioni, contestazioni di brevetti… Tale caratteristica non fa quindi altro che acuire la difficoltà di gestione del portafoglio tecnologico e, di conseguenza, rendere maggiormente complessa l'attuazione delle misure di adeguamento normativo e di sicurezza.

Anche dal punto di vista delle Apps, sono numerosi i player identificabili: dalle società produttrici di dispositivi stesse, mediante società satelliti, a società dedicate, a *software integrator*, a soluzioni realizzate autonomamente in ambito aziendale (e quindi in ambito *trusted*). In alcuni casi i prodotti rilasciati da tali soggetti sono sottoposti a processi approvativi (più o meno rigidi) da parte delle piattaforme che li ospitano, in altri casi invece le Apps non sono soggette a verifiche di qualità e di sicurezza del software, potendo pertanto costituire dei notevoli rischi potenziali.

Ulteriori aspetti di utilizzo rilevanti

A completamento del breve contesto di riferimento si evidenziano di seguito alcuni trend che introducono elementi rilevanti ai fini della compliance e della sicurezza.

Il primo elemento fa riferimento ad un approccio di recente formulazione in alcuni contesti aziendali, ovvero quello che è definito *Bring Your Own Device* (di seguito BYOD): tale approccio parte dal presupposto che gli utenti sono così abituati alle funzionalità del dispositivo da loro preferito che il suo utilizzo anche in ambito lavorativo potrebbe potenzialmente fornire benefici produttivi. Pertanto l'utente sceglie il dispositivo, lo stesso utente o la società lo mette a disposizione e le società forniscono i servizi alla base dei processi di business correlati (e.g. connettività, raggiungimento di dati ed informazioni, servizi infrastrutturali…).

Pur presentando potenziali benefici in termini di operatività, tale approccio genera necessariamente anche alcuni potenziali rischi di sicurezza e di compliance, tra i quali (soprattutto ai fini del presente documento), la perdita di governo diretto sui dispositivi e, quindi, potenzialmente, anche delle misure di protezione correlate. Ciò comporta che, affinché siano garantiti gli opportuni livelli di sicurezza dei dati e delle informazioni trattate, le misure di protezione devono essere attestate direttamente sui servizi di cui si avvalgono gli utenti.

Ad esempio se con il dispositivo si vogliono utilizzare le possibilità di connettività aziendali, è necessario che i meccanismi di autenticazione alla rete aziendale prevedano anche elementi integrativi di verifica, quali, ad esempio, la configurazione del dispositivo, la presenza di software antimalware aggiornato o che impediscano la contemporanea presenza di connessioni diverse, che possano creare problematiche di *bridging*.

Il secondo elemento, correlato e parzialmente sovrapposto al primo è quello dell'utilizzo promiscuo dei dispositivi in ambito aziendale. A prescindere dall'attuazione di approcci BYOD, infatti, come anche previsto dall'Autorità Garante nelle linee guida del 01.03.2007 sulla gestione dell'email e della navigazione Internet in ambito aziendale, sempre più spesso gli strumenti assegnati per fini lavorativi sono utilizzati anche per fini personali. Secondo le suddette linee guida, l'approccio consigliato, in virtù dei pronunciamenti giurisprudenziali contrastanti, non è quello di consentire un uso solamente lavorativo (anche perché in molti casi i dispositivi sono forniti ai dipendenti in qualità di benefit e di semplici asset aziendali), ma di prevedere opportune regole, affinché l'uso personale sia limitato a modalità e casistiche ben definite (condivise sia con il dipendente che, con le rappresentanze sindacali) e assogettarne la contravvenzione a sanzioni disciplinari.

Ultimo elemento di contesto che si vuole presentare è quello dei possibili impieghi che nel futuro prossimo, di tali dispositivi. Di sicura rilevanza è quello correlato all'impiego della tecnologia Near Field Communication, ovvero su quelle soluzioni tecnologiche basate su connettività wireless a corto raggio e sviluppata congiuntamente da Philips, Sony e Nokia. NFC, contrariamente ai più semplici dispositivi RFID, permette una comunicazione bidirezionale: quando due apparecchi NFC (l'Initiator e il Target) vengono accostati entro un raggio di 4 cm, viene creata una rete peer-to-peer tra i due ed entrambi possono inviare e ricevere informazioni. I possibili utilizzi già realizzati, sia in via sperimentale che a supporto di modelli di business, possono riguardare esempi quali:

- l'acquisizione ed il pagamento su dispositivi portatili NFC, attraverso computer o chioschi elettronici abilitati, di servizi, giochi, file MP3, video, software;
- acquisizione da un computer su di un dispositivo portatile, della prenotazione o acquisto di una permanenza in albergo, ingressi a cinema, teatri, stadi, viaggio in treno o aereo, ed accesso al servizio comperato mediante il dispositivo stesso avvicinandolo o toccando il chiosco elettronico in albergo, al gate di ingresso o di partenza;
- acquisizione da un chiosco elettronico mediante scansione o contatto di informazioni addizionali, acquisto di una permanenza in albergo, ingressi a cinema, teatri, stadi, titolo di viaggio con mezzi urbani e accesso al servizio mediante il dispositivo stesso anche sui mezzi di trasporto urbano;
- trasferimento e visualizzazione di fotografie da una macchina fotografica o telefono cellulare NFC a un chiosco elettronico, televisione, computer per la visione o la stampa.

Inquadramento dei rischi di Privacy nel *Mobile*

Come evidenziato in precedenza, la rapida affermazione dell'adozione dei dispositivi mobili evoluti in ambito aziendale è dovuta sia ad una serie di aspetti di natura sociale e tecnologica, sia ad effettivi benefici che essi possono potenzialmente garantire, attraverso la realizzazione di un modello di "*mobile office*". Tra i maggiori benefici che tale modello può garantire, possono essere evidenziati:

- l'aumento della produttività, garantendo l'accessibilità alle informazioni a prescindere dalla specifica locazione fisica del dipendente (soprattutto se il modello è associato all'adozione di soluzioni e servizi di cloud computing);
- la possibilità di erogare nuovi servizi ai clienti, basati su una maggiore reperibilità e disponibilità delle informazioni;
- l'attivazione di nuove forme di comunicazione a livello aziendale ;
- l'accesso tempestivo e contestualizzato alle applicazioni aziendali con conseguente miglioramento del processo decisionale.

Ovviamente a fronte di tali benefici, l'adozione di tali dispositivi determina altresì l'introduzione di nuovi elementi di rischio e/o l'enfatizzazione di tipologie di rischio già esistenti in ambito aziendale, ma con elementi peculiari tipici di questo nuovo contesto tecnologico. Affinché tali rischi siano opportunamente governati, il Gruppo di lavoro ritiene fondamentale un approccio metodologico basato almeno su tre fasi principali, in linea con quanto evidenziato anche dallo standard di sicurezza ISO-IEC27001:

- l'identificazione e la classificazione dei trattamenti e dei dati;
- l'analisi dei rischi;
- il trattamento dei livelli di rischio determinati.

L'identificazione e la classificazione dei trattamenti e dei dati

Preliminarmente all'attuazione dell'analisi dei rischi, il Gruppo di Lavoro ritiene necessario ed opportuno che siano promosse:

- l'identificazione dei trattamenti effettuati mediante tali dispositivi;
- l'identificazione degli elementi tecnologici sottostanti ai trattamenti;
- l'identificazione dei dati trattati;
- la loro classificazione, in termini sia normativi che in relazione alla criticità dal punto di vista della sicurezza (in termini di riservatezza, integrità e disponibilità).

Tali attività, caratteristiche di qualsiasi ambito tecnologico, nonché esplicitamente richieste anche dallo standard ISO-IEC27001 e dalla normativa Privacy vigente[9], possono essere particolarmente rilevanti per l'ambito *mobile*, ma allo stesso tempo anche particolarmente complesse, in relazione ad alcuni aspetti evidenziati in precedenza, quali:

- l'utilizzo promiscuo dei dispositivi (personale e professionale), che determina la presenza contemporanea di dati di titolarità della società e dati che non lo sono (ad esempio quelli personali degli utenti);
- l'affermazione delle politiche di BYOD, che rendono particolarmente difficoltoso, se non opportunamente presidiato attraverso processi strutturati, l'identificazione delle tipologie di dispositivi utilizzati e le caratteristiche tecnologiche correlate (e.g. versioni OS installate, dispositivi di memoria presenti…)
- l'estensione del tracciamento delle informazioni, non soltanto ai soli dispositivi, ma anche a tutti gli elementi infrastrutturali correlati, che possono introdurre delle minacce per i dati trattati. Si pensi ad esempio ad una possibile gestione dei dispositivi che determini il salvataggio dei dati ad elementi centralizzati, spostando pertanto il focus dell'elemento tecnologico oggetto del rischio.

[9] Il tracciamento dei trattamenti e dei dati correlati, pur essendo stato rilassato a livello di formalizzazione del DPS, mediante la pubblicazione in G.U. del D.L.5/2012 (c.d. decreto "semplificazioni"), è comunque uno degli elementi obbligatori e necessari al fine di una corretta impostazione dell'attivazione dei trattamenti e di protezione dei dati.

Risulta dunque necessario innanzitutto che l'azienda effettui un puntuale tracciamento dei suddetti elementi, con l'obiettivo di comprendere meglio natura e livello del rischio ed interventi necessari per limitarne gli impatti.
A fronte di tale tracciamento poi tali trattamenti ed i dati correlati dovrebbero essere opportunamente classificati in termini di criticità di *sicurezza e compliance*.

L'analisi dei rischi per i trattamenti di dati personali effettuati mediante dispositivi mobili evoluti

L'analisi dei rischi ha come oggetto la determinazione dei livelli di rischio, a cui sono esposti i trattamenti ed i dati correlati, attraverso una valutazione delle minacce che possono avere degli impatti su tali attività aziendali. Essa può essere condotta seguendo diverse metodologie, derivanti da standard e *best practice* di settore ovvero proprietarie, che si possono differenziare sulla base di:

- approcci metodologici complessivi (in alcuni casi sono considerate le specifiche minacce, in altre si prendono in considerazione le vulnerabilità…)
- elenco delle minacce prese in considerazione;
- metriche di misurazione del rischio;
- aspetti correlati al processo di realizzazione (ripetibilità, frequenza, responsabilità…).

Tutte le diverse metodologie sono universalmente applicate ai diversi contesti tecnologici ed operativi, con vantaggi e criticità specifiche; ciononostante, nell'ambito dei trattamenti di dati personali effettuati mediante utilizzo dei dispositivi mobili evoluti esistono degli elementi di rischio di particolare significatività, di seguito analizzati, correlati sia alle specifiche minacce che alle correlate vulnerabilità sottostanti.

Rifacendosi all'elenco proposto dall'Autorità Garante per la predisposizione dei DPS, il Gruppo di Lavoro ritiene che nella realizzazione delle analisi debbano essere prese in considerazione, almeno le tipologie di rischio di seguito indicate, opportunamente analizzate nel contesto *mobile*.

Rischi di sicurezza dei dati trattati correlati ai comportamenti degli utilizzatori

La prima tipologia di rischio è quella correlata all'uso che gli utilizzatori fanno dei dispositivi mobili. Le analisi di rischio relativamente a tale tipologia dovrebbero considerare le seguenti casistiche:

- errori materiali nell'effettuazione dei trattamenti, quale ad esempio l'invio di una mail a destinatario erroneo o l'errata condivisione di documentazione con soggetti non autorizzati;
- gestione impropria delle credenziali di accesso al dispositivo / ai servizi;
- gestione impropria dei servizi presenti sul dispositivo, ad esempio attraverso l'apertura di servizi sul telefono che determinino delle vulnerabilità di sicurezza;
- accesso a servizi di particolare criticità, quali *social network;*
- (nel caso principalmente di smartphone) comunicazioni vocali non sicure, ovvero *disclosure* di informazioni critiche e dati sensibili in ambienti pubblici;
- comportamenti sleali o fraudolenti degli operatori, correlata ad esempio all'utilizzo del dispositivo per sottrarre indebitamente del materiale aziendale.

Fatta eccezione per l'ultima casistica, generalmente indirizzata da opportune misure organizzative, procedurali e tecnologiche, uno degli elementi alla base dei restanti rischi è correlabile alla mancanza di consapevolezza dei rischi da parte degli utilizzatori dei dispositivi. Considerata la destinazione promiscua (personale e lavorativa) che generalmente caratterizza i dispositivi, sarebbe pertanto consigliabile attivare in merito un programma di sensibilizzazione *ad hoc* sul corretto utilizzo dei dispositivi[10], soprattutto mediante iniziative formative.

[10] In tal senso si veda il capitolo seguente correlato agli adempimenti formali.

Altro elemento di primaria rilevanza per il trattamento di tali rischi è la creazione di policy aziendali e di linee guida in cui siano identificati e tenuti in considerazione tutti i possibili rischi che possono derivare dall'utilizzo dei dispositivi mobili definendo opportune regole di comportamento che gli utilizzatori devono seguire e dettagliando responsabilità individuali e di ruolo al fine di garantire protezione e sicurezza dei dispositivi mobili e dei dati in esso contenuti.

Poiché l'utilizzo promiscuo dei dispositivi mobili per finalità sia private che lavorative determina la presenza di diverse tipologie di dati su tali dispositivi, si rende necessaria una chiara regolamentazione dei dispositivi in termini di classificazione dei dati al fine di identificare e minimizzare l'impatto che lo smarrimento o il furto dei dispositivi stessi potrebbe comportare.

Rischi di sicurezza dei dati trattati correlati agli strumenti

I dispositivi mobili evoluti, come visto in precedenza, sono caratterizzati da notevoli capacità computazionali, di memoria e dalla possibilità di connettersi a diversi servizi telematici offerti in ambito aziendale[11]. Gli utenti possono infatti utilizzare applicazioni, memorizzare o modificare dati provenienti dal network aziendale o da Internet.

Queste caratteristiche tecnologiche determinano ovviamente dei rischi di carattere prevalentemente tecnologico quali:

- azione di virus informatici o di programmi suscettibili di recare danno;
- spamming o tecniche di sabotaggio;
- malfunzionamento, indisponibilità o degrado degli strumenti;
- attivazione di accessi esterni non autorizzati;
- intercettazione di informazioni in rete;
- danneggiamento dei dispositivi.

Tali rischi possono essere correlati ad elementi di vulnerabilità, quali la non corretta configurazione dei dispositivi / dei servizi correlati, la mancata applicazione di *patching* pubblicate, la mancata adozione preventiva di misure di protezione (sistemi antimalware, sistemi perimetrali di protezione…), il limitato controllo sulle Apps accessibili ed installabili sui dispositivi…

Dato il drammatico aumento delle Apps disponibili, soprattutto quest'ultimo elemento può essere causa di notevoli problemi di sicurezza sui dati trattati.
Anche i rischi correlati alle minacce malware sono particolarmente rilevanti e di attualità: tenuto in considerazione anche che l'adozione di sistemi antimalware sui dispositivi mobili è ancora molto limitata risultano infatti particolarmente critici gli aspetti di esposizione rispetto a virus, worm[12] …

Il pericolo di "hacking" (accesso non autorizzato) e di "sniffing" (intercettazione di informazioni) è poi particolarmente elevato utilizzando dispositivi mobili. Date infatti le caratteristiche tecnologiche di alcune piattaforme, un soggetto ostile potrebbe sfruttare eventuali falle e vulnerabilità di sicurezza per accedere e acquisire impropriamente i dati personali contenuti all'interno del dispositivo o accessibili attraverso lo stesso.

Infine, relativamente alla disponibilità delle informazioni, anche i guasti dei dispositivi sono un elemento da tenere in considerazione: i dispositivi mobili, infatti, essendo di piccole dimensioni e facilmente trasportabili, possono incorrere più frequentemente in urti e danni esterni.

[11] Nel caso degli smartphone tali caratteristiche si aggiungono a quelle di funzionalità telefoniche vere e proprie, anche se con gli attuali servizi VOIP, tale separazione si sta sempre più assottigliando).

[12] Tali dispositivi sono soggetti ad un determinato tipo di virus, il "Mobile Worm". Un worm ha la capacità di modificare il dispositivo che infetta in modo da venire eseguito ad ogni avvio. Il mezzo più comune per la sua diffusione è la posta elettronica. Un mobile worm può ricercare indirizzi e-mail memorizzati nel dispositivo ospite ed inviare una copia di sé stesso come file allegato (attachment) a tutti o parte degli indirizzi che riesce a raccogliere.

Rischi di sicurezza dei dati trattati correlati al contesto fisico-ambientale

Tali tipologie di rischio sono apparentemente quelle maggiormente percepite da parte dei soggetti. I primi elementi di rischio citati infatti in ambito *mobile*, a ragion del caso, sono generalmente quelli di furto o smarrimento del dispositivo.
Prendendo però in considerazione l'elenco completo delle tipologie di rischio anche indicato dal Garante Privacy nel contesto dell'analisi per finalità di redazione del DPS, il Gruppo di Lavoro ritiene che i rischi da considerare vadano però oltre tali casistiche semplificate. In tal senso i principali eventi da tenere in considerazione sono:

- sottrazione o smarrimento dei dispositivi contenenti i dati/servizi che permettono l'accesso ai suddetti;
- eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali), nonché dolosi, accidentali o dovuti ad incuria;
- guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.);
- errori umani nella gestione della sicurezza fisica.

Come detto il rischio legato alla sottrazione o allo smarrimento dei dispositivi è quello maggiormente percepito e di fatto più probabile, sulla base della quantità di incidenti più o meno rilevanti segnalati in tal senso. A meno dell'attuazione di misure di protezione dei dati, illustrate nei capitoli seguenti, tale evento è correlato al rischio di un successivo accesso non autorizzato a dati e informazioni critiche e/o alla perdita degli stessi.
I restanti eventi, a prima vista sembrerebbero poco correlati all'ambito dei dispositivi mobili, data la loro peculiarità principale di non essere correlati ad una specifica sede fisica. In realtà, una corretta analisi del contesto dei trattamenti, mediante dispositivi mobili, dovrebbe tenere in considerazione, non solo gli elementi terminali, ma anche tutti gli elementi infrastrutturali centralizzati. Si pensi ad esempio infatti al crollo di un CED contenente i server BES per una piattaforma Blackberry: seppure tale evento non abbia un impatto diretto sui terminali esso di fatto potrebbe rendere indisponibili i servizi ed i dati, azzerando quindi i vantaggi offerti dal modello di *"mobile office"*. Lo stesso tipo di ragionamento ovviamente vale non solo per eventi disastrosi, ma altresì per la mancanza di infrastrutture complementari (energia elettrica, condizionamento…).

Rischi correlati a trattamenti non conformi alle normative e/o alle policy aziendali

La realizzazione di trattamenti di dati personali mediante i dispositivi mobili evoluti in ambito aziendale può riguardare anche rischi non strettamente correlati ad aspetti di sicurezza dei dati e delle informazioni trattate, quanto alla correttezza ed alla conformità dei suddetti trattamenti. Si pensi ad esempio ad un trattamento che, pur essendo realizzato mediante l'adozione di tutte le misure di protezione necessarie (minime, obbligatorie ed idonee, secondo lo schema di seguito presentato), non risponda ai requisiti formali di una normativa applicabile (in questo caso la normativa Privacy). Ecco che, pur non determinando particolari impatti sui parametri RID[13] di sicurezza, il trattamento potrebbe comportare degli impatti di tipo legale (sanzioni…), reputazionale ed anche economico. Un caso significativo, in tal senso, è stato quello di una ben nota società del settore TLC di respiro internazionale che, pur garantendo tutti gli aspetti di sicurezza del caso, acquisiva dei dati di localizzazione del terminale, senza averne mai informato gli utenti.

Elementi di particolare rilevanza da tenere in considerazione quali minacce / eventi che possono essere significativi per tale tipologia di rischi nell'ambito *mobile* includono:

- mancata notificazione per l'acquisizione ed il trattamento di dati soggetti a tale processo;
- mancata segnalazione nelle informative verso i dipendenti (in qualità di interessati), o di ulteriori soggetti dell'eventuale effettuazione di trattamenti correlati all'utilizzo dei dispositivi;
- mancata acquisizione del consenso per il trattamento di particolari dati (giudiziari, sensibili) e/o per l'effettuazione di particolari trattamenti, anche su dati non partico-

[13] Riservatezza, Integrità e Disponibilità.

larmente critici in sé e per sé (si pensi ad esempio all'eventuale analisi delle abitudini dei propri dipendenti in merito alla navigazione in siti della società per determinare la validità dei contenuti offerti dai propri portali…);
- mancata fornitura di istruzione agli incaricati relativamente ai loro obblighi ed alle loro responsabilità in merito all'utilizzo dei suddetti dispositivi.

Si badi bene che l'indicazione non è correlata al fatto che le attività evidenziate non possano essere realizzate (nel qual caso si eliminerebbe il rischio), ma che le stesse siano realizzate nel mancato rispetto della normativa vigente.
Allo stesso tempo poi, soprattutto nei contesti dei grandi gruppi internazionali, l'utilizzo di tali dispositivi nel mancato rispetto delle normative interne (a volte più restrittive di quelle normative), può altresì comportare significativi impatti (e.g. si pensi ad esempio al mancato rispetto di prassi per la protezione di dati personali che ai fini Privacy possano essere ritenuti non critici – e.g. le anagrafiche di fornitori – ma che lo siano ai fini di business), quali multe, perdita di controllo su specifiche attività…

Come illustrato in precedenza, tanto le cause, quanto gli impatti delle suddette tipologie di rischio possono essere strettamente correlati a specifiche vulnerabilità intrinseche dell'ambito aziendale quali:
- il mancato governo delle normative cogenti, relativamente alle attività realizzate con i dispositivi;
- l'attitudine al rispetto delle normative interne comportamentali da parte del personale;
- l'inclusione nelle operatività aziendali di soggetti terzi, non allineati sulle normative interne / su quelle esterne applicabili;
- il mancato presidio sul portafoglio tecnologico;
- la complessità del contesto tecnologico che può rendere intrinsecamente difficoltoso governare tutti gli aspetti di sicurezza.

Ulteriori tipologie di rischio da considerare

Trasversalmente alle tipologie precedenti, il Gruppo di Lavoro evidenzia la forte necessità di tenere sotto controllo e gestire anche gli aspetti di rischio derivanti dall'affidamento in outsourcer delle infrastrutture e/o dei trattamenti.
Laddove infatti molte delle funzionalità offerte dai dispositivi mobili siano gestite da un outsourcer, l'azienda non dovrà solo implementare contromisure al fine di gestire il rischio gravante sui propri asset, ma dovrà altresì assicurarsi che gli outsourcer implementino opportune contromisure per minimizzare e gestire il rischio derivante dalle minacce applicabili ai dati ed alle informazioni trattate.

L'importanza di tale aspetto è stata recentemente evidenziata da un incidente occorso all'infrastruttura centralizzata di una delle maggiori piattaforme di dispositivi cellulari per l'ambito aziendale, che, a causa di un incidente nella realizzazione di interventi di manutenzione evolutiva/ di upgrading dei sistemi, ha comportato una lunga indisponibilità dei servizi offerti su dispositivi mobili e pertanto gravi impatti sui servizi e sui trattamenti di dati personali.

Le tipologie di impatto

L'accadimento di uno degli specifici eventi correlati alle diverse tipologie di rischio evidenziate in precedenza determina degli impatti a livello aziendale, generalmente classificabili nelle seguenti tipologie:
- impatti economici, sia diretti che indiretti relativi all'accadimento dell'evento. Mentre gli impatti diretti sono generalmente molto semplici da stimare (e.g. valore del dispositivo perso, valore dell'infrastruttura centralizzata attaccata…), quelli indiretti possono essere di ben difficile determinazione. Si pensi ad esempio allo smarrimento di un dispositivo ed ai valori attribuiti alle informazioni contenute e/o alla necessità di ricostruire eventuali contesti informativi, qualora non opportunamente salvati in infrastrutture centralizzate. In tal senso possono essere di significativo supporto delle stime preventi-

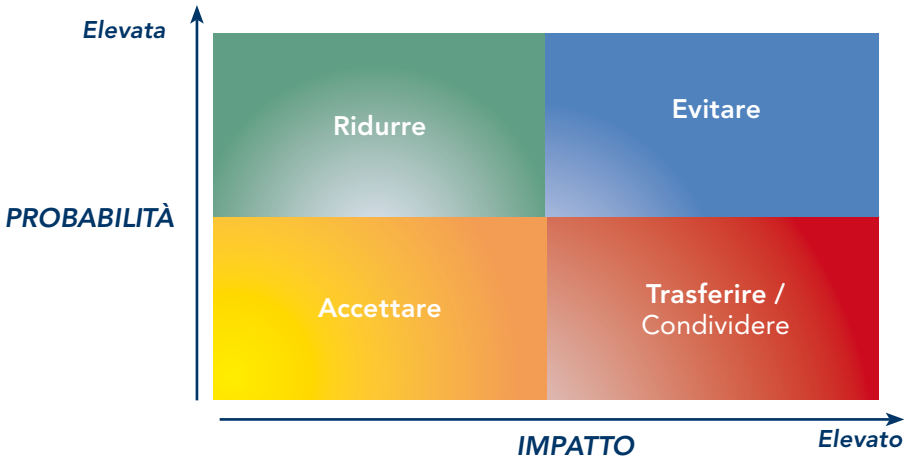
ve relative al rapporto "importo degli interventi di sicurezza" / "benefici attesi[14]";
- impatti di immagine/reputazionali. Tale tipologia, spesso sottovalutata, all'atto di valutare la necessità di investimenti in sicurezza e compliance (a favore ad esempio di quelli economici e normativi di più facile determinazione), è in molti casi quella di maggiore rilevanza, soprattutto in relazione a contesti tecnologici avanzati e/o a servizi offerti verso soggetti aziendali, basati in molti casi su relazioni di *trust*. In tali casi infatti è possibile considerare che l'accadimento di un solo evento sia in grado di minacciare la complessiva continuità aziendale;
- impatti normativi, ovvero gli impatti correlati ad aspetti legali (litigation, …) e/o di non compliance normativa (sanzioni, blocco dei trattamenti…);
- impatti sulla competitività, ovvero quegli impatti che a causa dell'evento possono inficiare in modo diretto la capacità competitive della società di esse.

Tali impatti sono ovviamente fortemente correlati allo specifico contesto operativo e settoriale.

Le attività di trattamento dei livelli di rischio determinati

In seguito alla realizzazione dell'analisi dei rischi e della determinazione dei livelli correlati ai vari eventi di rischio specifici, è necessario che si proceda a gestire opportunamente i livelli di rischio individuati (c.d. "trattamento del rischio") per portarli a situazioni ritenute accettabili dalla società. Anche in tale caso, le attività correlate, fanno riferimento ad approcci metodologici ben consolidati, le cui strategie si muovono su quattro linee generali ovvero l'accettazione del rischio, il suo trasferimento, la mitigazione/riduzione e l'eliminazione (evitandolo).

Figura 2
Lo standard ISO27001 e l'implementazione di un SGSI Approccio Risk-Based



Ciononostante per tutti gli aspetti visti in precedenza, si ritiene che l'attuazione delle suddette strategie in ambito *mobile* sia da declinarle opportunamente, come di seguito evidenziato:

- **accettazione del rischio**, ovvero la scelta della società di non effettuare ulteriori iniziative di trattamento approvando (consapevolmente) il livello di rischio riscontrato. I criteri di accettazione del rischio o per identificare i livelli di rischio che organizzazione ritiene accettabili dovrebbero essere definiti contestualmente all'identificazione della metodologia da utilizzare per la valutazione dei rischi derivanti dall'utilizzo di dispositivi mobili. Accettando il livello di rischio individuato durante il processo di valutazione, l'organizzazione valuta che quei rischi siano compatibili con i criteri adottati e, di conseguenza, che non sia necessario implementare alcuna azione di mitigazione o trasferimento del rischio. Ma, tenendo in considerazione quanto evidenziato nei precedenti capitoli, rimangono aperte alcuni elementi di riflessione:
  – quanto le società possono essere e sono pienamente consapevoli e coscienti degli

[14] Si veda in tal senso anche quanto sviluppato da un GDL precedente relativamente al ROSI, ovvero alle valutazioni sui ritorni degli investimenti in sicurezza. Rif. http://rosi.clusit.it/pages/Homepage.html

elementi tecnologici, dei dati e dei servizi erogati e di tutte le caratteristiche correlate, al fine di determinare la decisione maggiormente opportuna?
  - Come affrontare la decisione di accettazione del rischio, quando le scelte delle modalità di trattamenti dei dati e degli elementi tecnologici correlati sono realizzate in alcuni casi dagli utenti e/o possono essere eventualmente governati attraverso l'imposizione di indicazioni comportamentali, ma senza il diretto governo?
- **trasferimento e condivisione del rischio**, relativa alla linea strategica di estendere il livello di rischio individuato ad un soggetto terzo. Tipicamente il soggetto terzo è rappresentato da una società assicurativa (attraverso una stipula di apposite polizze che coprano i possibili impatti) e/o da outsourcer (a cui, tramite sottoscrizione di contratti, viene demandata la gestione dello specifico rischio). Premesso che la scelta di effettuare il trasferimento del rischio ad soggetto terzo ed esterno alla società non comporta il contestuale trasferimento delle relative responsabilità, che rimangono comunque in capo all'organizzazione stessa, l'implementazione della linea è comunque soggetta, in ambito mobile ad una serie di considerazioni quali:
  - è possibile il trasferimento del rischio anche in contesti operativi dove non è possibile delineare puntualmente gli elementi di contorno (e.g. se i dispositivi sono scelti e gestiti dai dipendenti), soprattutto se non è attuato un processo di governo e gestione strutturato dei trattamenti effettuati con tali dispositivi?
  - A chi compete il trasferimento del rischio se i dispositivi sono di proprietà di soggetti terzi (si pensi ad esempio ad agenti di una forza vendite o a dei rappresentanti)?
  - Quali costi intrinseci correlati a tali aspetti possono essere evidenziati da soggetti che si assumano il rischio e quali elementi di misurazione di benefici/costi possono essere adottati in merito?
- **eliminazione del rischio**, consistente nell'approccio, forse meno difficoltoso dal punto di vista attuativo, consistendo nell'eliminazione dell'elemento che determina il rischio correlato, però più impattante dal punto di vista operativo: la rinuncia all'elemento centrale, ovvero il trattamento di dati tramite dispositivi mobili evoluti, comporta infatti inevitabilmente anche la rinuncia a tutti i benefici correlati all'introduzione del modello di "mobile office" e dovrebbe essere quindi presa in considerazione solamente nel caso in cui gli impatti superino largamente gli stessi benefici;
- **mitigazione del rischio**, ovvero l'individuazione e l'attuazione di opportune misure di natura organizzativa, procedurale e tecnologica, volte a ridurre il livello di rilevato. La selezione ed implementazione delle misure deve tener conto dello specifico contesto operativo e dei necessari vincoli esistenti di tempo, di budget, tecnici, culturali e legali. Tipicamente la linea di mitigazione del rischio si può articolare in:
  - misure di riduzione del rischio ossia controlli ed obiettivi di controllo che agiscono sulle cause che determinano la presenza del rischio individuato, comportando di conseguenza una diminuzione della probabilità di accadimento;
  - misure di mitigazione del rischio ossia controlli ed obiettivi di controllo che agiscono sugli effetti che il rischio individuato può comportare, diminuendo di conseguenza l'impatto che ne può derivare.

Al fine di facilitare la scelta di misure che si ritengono idonee per la riduzione significativa del rischio in ambito *mobile*, si riportano in un successivo capitolo dedicato, quelle che vengono ritenute di maggiore rilevanza. Ovviamente la pertinente adozione delle misure idonee è subordinata alla corretta analisi del contesto ed ai risultati dell'analisi dei rischi.

Inoltre l'analisi dei rischi e l'adozione delle misure di sicurezza devono essere strettamente correlate alle strategie aziendali di business e a quelle più specifiche dell'evoluzione dei sistemi e dei servizi IT.

Inquadramento degli aspetti giuridici e legali

Premessa

Uno degli aspetti di rischio maggiormente rilevante e che deve essere, pertanto, opportunamente indirizzato è quello della non conformità normativa nell'effettuazione dei trattamenti di dati personali attraverso dispositivi mobili evoluti adottati (o da essi generati).
Affinché tale rischio sia opportunamente indirizzato è preliminarmente necessario identificare i risvolti legali correlati, con particolare attenzione agli adempimenti formali, di seguito analizzati.
Tale analisi verterà principalmente sulla normativa Privacy vigente, (Codice Privacy e provvedimenti correlati), per poi analizzare brevemente gli ulteriori contesti normativi applicabili all'ambito di indagine.

La normativa Privacy e i principali adempimenti formali

La normativa in tema di Privacy è volta a garantire il corretto trattamento dei dati personali nel rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'individuo con riferimento, in particolare, al diritto alla riservatezza, garantendo l'adozione di opportune misure di sicurezza preposte a tale fine.
Tuttavia, come si vedrà anche nei successivi capitoli dedicati alle misure di sicurezza, le attuali indicazioni normative sono pensate e, quindi, applicabili e correlabili a strumenti elaborativi tradizionali, richiedendo uno sforzo esegetico ed interpretativo affinché esse possano essere riferite allo specifico ambito dei dispositivi mobili.

La necessità di integrazione con l'attuale normativa è altresì testimoniata dal recente intervento dell'Autorità Garante dei dati personali che, mediante la pubblicazione delle "linee guida" su smarthphone e tablet, ha posto l'attenzione sugli aspetti critici correlati a tali dispositivi, fornendo indicazioni per un corretto e consapevole utilizzo degli stessi[15].
La rilevanza di tale aspetto è stata confermata anche durante l'ultima conferenza italiana sulla sicurezza informatica (Security Summit 2011) in cui è stato evidenziato come l'impatto delle Apps sulla sicurezza delle telecomunicazioni in cui oltre il 20% delle applicazioni esistenti avrebbe accesso a informazioni private o sensibili dell'utente: le applicazioni, infatti, in alcuni casi hanno la possibilità di accedere a dati e strumenti (per esempio numero di telefono, rubrica, messaggi) in un modo ancor più invasivo che in passato e rispetto ad altri strumenti.

L'adozione dei dispositivi mobili evoluti nella realizzazione di trattamenti di dati personali in ambito aziendale comporta la necessità di adeguarsi a diversi adempimenti formali richiesti da tal contesto normativo (Codice Privacy e provvedimenti specifici).

Nel considerare tali adempimenti è bene tenere in considerazione che il quadro complessivo, riassunto nella Figura 3, è soggetto a specifiche variazioni, relative a:

- tipologie di dati trattati (ad esempio: dati di salute, dati relativi all'ubicazione, …);
- potenziali utilizzi dei dati (ad esempio: marketing, fornitura di un servizio richiesto dall'interessato, …);
- particolari settori (ad esempio: telecomunicazioni, assicurazioni, banche, …);
- possibilità o meno di raccogliere il consenso (in analogia a quanto previsto dall'Autorità Garante Privacy per i trattamenti dei dati di videosorveglianza).

[15] In particolare il Garante evidenzia "I rischi connessi agli smartphone e alle loro applicazioni derivano essenzialmente dal fatto che i nostri telefonini sono costantemente localizzati, e che il gran numero di dati e informazioni in essi contenuti, dalle rubriche telefoniche all'agenda, dalle foto alle annotazioni, possono essere conosciuti, trattati, conservati, utilizzati da soggetti dei quali non abbiamo consapevolezza né controllo. Pensare al rischio di essere controllati immaginandosi ancora l'uomo con la cuffia che ascolta le conversazioni, o credere che il solo rischio per la libertà di comunicazione e di circolazione sia che qualcuno possa intercettare le nostre telefonate o gli sms, o localizzare gli spostamenti acquisendo i tabulati dei dati di traffico telefonico, è come pensare che la scoperta più recente dell'umanità sia la macchina a vapore. La realtà è ben diversa. Con gli smartphone ognuno di noi è, quasi sempre inconsapevolmente, un Pollicino che ha in tasca il suo sacchetto di sassolini bianchi che escono uno ad uno per segnarne gli spostamenti. Peraltro la geolocalizzazione è solo uno degli effetti di un sistema di interconnessioni che può essere utilizzato con modalità e conseguenze diversissime, in una galassia di applicazioni che si moltiplica ogni giorno e delle quali spesso non si conoscono le implicazioni".

Sulla base di tali elementi variabili potranno applicarsi diversi provvedimenti dell'Autorità, che possono comportare diverse prescrizioni sia formali sia di sicurezza… Ad ogni buon conto, gli adempimenti universalmente validi possono essere così sintetizzati.

Figura 3
Sintesi degli adempimenti universalmente validi

A tali adempimenti occorre aggiungere che, se il trattamento risulterà realizzato in diversi paesi dell'Unione Europea (ma questo avverrà a maggior ragione verso paesi extra-UE), occorrerà individuare gli adempimenti specificamente richiesti da ciascuna normativa. In alternativa è possibile individuare la più restrittiva e adeguarsi ad essa divenendo "necessariamente" compliant con le altre[16].

Fatta eccezione per le misure di sicurezza, analizzate dettagliatamente nei capitoli dedicati, di seguito si analizzano brevemente tali adempimenti formali, cercando di evidenziarne gli elementi peculiari in relazione ai trattamenti fatti con i dispositivi mobili evoluti.

Gestione delle informative e dei consensi

Dal punto di vista dei trattamenti di dati personali mediante dispositivi mobili evoluti, l'adempimento formale correlato alla gestione delle informative e dei consensi ha una doppia lettura. Mentre, infatti, i trattamenti, operati mediante tali dispositivi, relativi a dati di soggetti esterni (clienti, fornitori), non sono generalmente specificati nelle informative loro fornite in quanto non dovrebbero comportare specifici adempimenti formali (a meno di trattamenti particolari), oltre a quelli generalmente previsti (informativa, consenso, misure di sicurezza…), quelli correlati a dati afferenti al personale (dipendenti, collaboratori) potrebbero comportare l'esigenza di adempimenti aggiuntivi e/o specifici.

Tali integrazioni dovrebbero riguardare i trattamenti di dati che scaturiscono dall'utilizzo del dispositivo e che possono comportare la conservazione o l'analisi di informazioni relative al personale, nella sua veste di interessato (si pensi ad esempio al trattamento dei dati di navigazione o di utilizzazione dei servizi telefonici).

Data però la complessità degli aspetti da analizzare, il Gruppo di Lavoro evidenzia che, in tale contesto, i contenuti informativi potrebbero essere forniti ai dipendenti secondo due livelli:

- a livello di informativa vera e propria (secondo il normale schema normativo);
- a livello di *policy* utenti, in cui siano indicate le modalità ed i corretti utilizzi dei dispositivi e le ulteriori condizioni al contorno (possibilità di verifica progressiva dei dati generati…), così come già indicato dall'Autorità Garante Privacy nelle già citate Linee Guida del 01.03.2007 a proposito di e-mail e navigazione Internet.

[16] Naturalmente, all'interno dell'UE, questo approccio potrà mutare nei prossimi anni in virtù delle novità annunciate in termini sia di regolamento che di direttiva.

Informativa. Posto che il Codice Privacy, all'art. 13, indica con precisione quali elementi devono essere inclusi in un'informativa completa, nel caso di trattamenti operati in ambito *mobile*, non deve sfuggire che esistono servizi che sono offerti di *default* dai terminali e che possono comportare il trattamento o la conservazione di informazioni relative al dipendente (assegnatario del terminale), in una varietà di siti (intesi come luoghi fisici) differenti rispetto alla sede dell'azienda, ad esempio:

- il luogo dove l'azienda ha collocato la propria *server farm* (che non è necessariamente presso la sede operativa);
- il luogo dove è collocato il CED dell'operatore che fornisce la connettività;

Esistono poi dei servizi, connaturati ai terminali adottati, che complicano ulteriormente l'individuazione dei siti (coinvolti nel trattamento o utilizzati nello *storage* dei dati) da indicare nell'informativa. Questo vale, ad esempio, per gli utenti della piattaforma Blackberry i cui dati possono attestarsi sulle macchine della società RIM in territorio estero, oppure per i possessori di device Apple, in relazione all'introduzione del servizio iCloud o anche in molte altre situazioni.

Policy utenti. In aggiunta ai contenuti specificati all'art. 13, esistono alcuni aspetti, specificamente legati all'uso del *mobile device*, che non è possibile o non è consigliabile introdurre in un'informativa, dato che la renderebbero prolissa, poco chiara e inidonea al perseguimento dello scopo per cui è stata introdotta dal legislatore.

A rispondere a questa esigenza dovrebbe provvedere la suddetta *policy* utenti, che dovrebbe avere lo scopo di informare e di incrementare la consapevolezza (*awareness*) degli utenti/dipendenti illustrando: quali usi dei *device* siano consentiti, quali servizi o modalità di utilizzo possano consentire la raccolta di informazioni, a volte sensibili, quali controlli legittimi possano essere condotti dal titolare del trattamento e quali sanzioni possano essere irrogate nel caso di uso distorto degli strumenti assegnati. In questo tipo di policy (cui si fa riferimento nel capitolo dedicato alle misure idonee), sarà opportuno segnalare, tra l'altro, che:

- l'uso del browser implica la raccolta di informazioni nella cronologia e attraverso la funzione di autocompletamento (questo fatto è di immediata percezione nei browser per PC, ma negli smartphone può essere complesso per un utente base individuare il modo per azzerare la cronologia e le altre funzioni che raccolgono informazioni per velocizzare l'accesso ai siti e le visite successive);
- la semplice cancellazione di applicazioni, in genere, non cancella tutte le tracce dell'applicazione stessa ma solo le shortcut (evidenziando che la cancellazione operata sullo smartphone, comunque, funziona in maniera molto meno profonda rispetto alla funzione di disinstallazione disponibile sul PC);
- l'uso e la fruizione dei file multimediali, sullo smartphone, è di difficile "occultamento" anche utilizzando apposite applicazioni a tutela della Privacy (che spesso spostano o cifrano ma non cancellano);
- l'uso di applicazioni che implicano l'acquisizione di dati relativi all'ubicazione del terminale potrà indurre il tracciamento: delle tempistiche di movimento e dei luoghi a cui l'utente/dipendente ha avuto accesso (questa e altre ipotesi analoghe, andranno comunque regolate in virtù di quanto espresso, ad esempio, nel case study sulla georeferenziazione).

Occorrerà inoltre indicare anche in quali situazioni, oltre a quelle legate ai controlli a tutela del patrimonio aziendale, potrà verificarsi l'accesso (anche incidentale) alle informazioni personali, ad esempio in occasione degli interventi di manutenzione sia del *software* che dell'*hardware* presente sul *mobile device*.

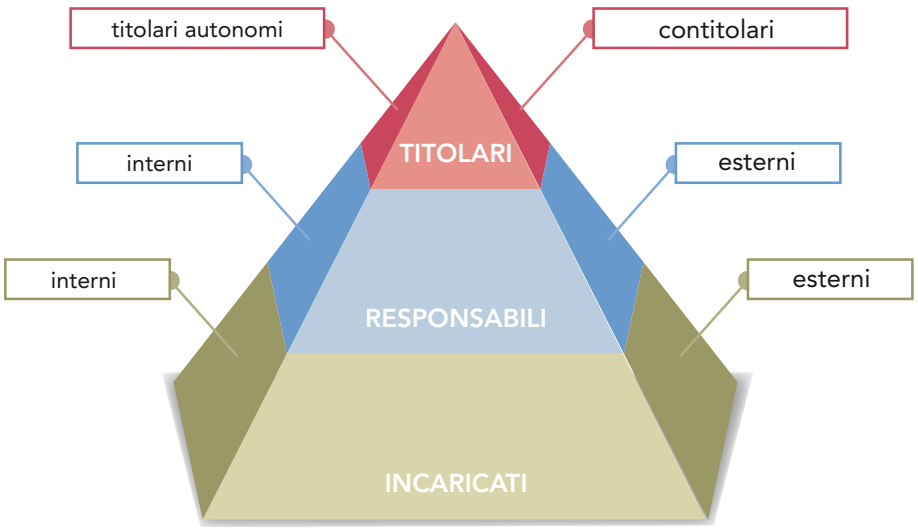
Infine si evidenzia un caso molto particolare, tipico però dell'ambito mobile, ovvero quelle delle Apps adottate in ambito aziendale. Nel caso infatti si promuovano /installino sui dispositivi in dotazione del personale delle Apps che (anche solo potenzialmente) acquisiscano e/o elaborino dati personali dei dipendenti o comunque degli utilizzatori dei dispositivi, dovrebbe essere verificato che tali trattamenti siano già coperti dalle informative fornite in precedenza a tali interessati e, in caso negativo, opportunamente prodotte apposite in-

formative (mediante canali tradizionali o mediante approcci innovativi, quali, ad esempio, pop-up al lancio dell'applicazione con accettazione delle condizioni).

Individuazione della titolarità e cotitolarità nei trattamenti, nomina e gestione dei responsabili e degli incaricati

Prendendo in considerazione la piramide dei "ruoli Privacy", illustrata nella figura che segue, occorre in primo luogo, considerare alcuni elementi caratteristici dell'ambito *mobile* che possono determinare anche situazioni caratteristiche distinte.

Figura 4
Piramide dei "ruoli Privacy"



In primis l'identificazione del titolare del trattamento, che non deve essere confuso con il/i soggetto/i, che in molti casi assumono ruoli di gestione tanto dei dispositivi, quanto dei servizi *mobile*. Si prenda ad esempio il caso di un titolare che effettui i trattamenti dei dati relativi alla posizione dei propri dipendenti per finalità ad esempio correlate all'ottimizzazione di servizi logistici e che tali trattamenti siano demandati ad un outsourcer esterno. Pur avendo un controllo solo parziale sull'operato dell'outsourcer, l'individuazione di quest'ultimo come titolare autonomo del trattamento, volta a scaricare le responsabilità su un soggetto terzo, resterebbe di difficile giustificazione di fronte all'Autorità. Ciononostante, le diverse situazioni configurabili non sono sempre di immediata e univoca interpretazione. Si consideri, ad esempio, un trattamento di dati personali, non direttamente acquisiti dalla società, ma dalla stessa trattati (e.g. dati di localizzazione offerti da alcuni tipi di piattaforme tecnologiche): l'attribuzione della titolarità in merito al suddetto trattamento potrebbe non essere di facile lettura realizzazione. Pertanto l'analisi della corretta titolarità del trattamento in ambito mobile, deve essere analizzata "caso per caso" in maniera attenta al fine di identificare gli effettivi perimetri di responsabilità e di titolarità dei suddetti trattamenti.

È bene comunque ricordare che anche l'attribuzione di contitolarità non è definizione vuota ma comporta un vero e proprio coordinamento tra le due (o più) entità (contitolari), al punto da far insorgere la possibilità che gli uni rispondano per la mancata adozione di misure di sicurezza da parte degli altri.

Infine, per completezza di analisi, si evidenzia che la "norma" che definisce il ruolo di "titolare dei dati" è scomponibile in tre elementi:

In particolare, in riferimento al secondo e terzo elemento, possiamo cogliere quanto la previsione del Gruppo ex art. 29 , indichi la possibilità che l'operazione (intesa come "macrotrattamento") possa essere messa in atto da un titolare autonomo oppure da uno o più contitolari, ma che comunque questi (i titolari o contitolari) vengano identificati in relazione al potere di condizionare le finalità dei trattamenti e le loro modalità di esecuzione.
Dunque anche in realtà multinazionali dove l'*outsourcer*, non di rado, è, a sua volta, una multinazionale ciò non comporta necessariamente che quest'ultimo venga identificato come autonomo "titolare del trattamento".

In completo disaccordo con gli orientamenti del gruppo ex art. 29[17], e anche alla lettera stessa della norma, il criterio spesso assecondato potrebbe essere definito "dimensionale", ovvero i titolari tendono ad individuare come titolare autonomo, l'outsourcer, in relazione al fatto che sia "troppo grande per poter essere controllato come responsabile del trattamento".
Viceversa occorre precisare che già il fatto di stabilire le finalità di un trattamento comporta la necessaria "subordinazione" dei soggetti che partecipino al trattamento stesso per perseguire la finalità individuata dal "controller" (ovvero dal titolare vero e proprio).

Applicando questi principi al nostro ambito ne consegue che **un'azienda che affidi, ad esempio, un servizio di fleet management o di tracking dovrà analizzare quanto abbia effettivamente delegato all'esterno e se il terzo operi, autonomamente, qualche trattamento rilevante (insomma non si limiti ad elaborare i dati "secondo le istruzioni ricevute").**
A seconda delle risposte che otterrà a tali quesiti potrà adeguatamente "individuare": titolari, contitolari, responsabili e incaricati.

Scendendo nella "piramide" titolare-responsabile-incaricati, questi ultimi (designati ex art. 30 del codice Privacy) sono caratterizzati da un atto di nomina particolarmente dettagliato e devono essere adeguatamente "formati" e "istruiti" per dare corretta esecuzione all'incarico ricevuto.

In particolare, il titolare del trattamento può prendere spunto, da quanto indicato dalla locuzione "attenendosi alle istruzioni impartite", di cui al comma 1 del citato art. 30, descrivendo con dovizia di particolari, non tanto l'attività che ciascun incaricato (o categoria di incaricati) è tenuto a svolgere, in quanto questo rientrerà più nei contenuti tipici di un mansionario, quanto come poter trattare i dati prodotti da o riferiti all'uso degli strumenti *mobile* e le implicazioni collegate in caso di incrocio di informazioni (ma anche di semplice accesso alle informazioni indicate) quali: i dati di ubicazione, il codice identificativo del terminale, i destinatari delle comunicazioni (...).
Pertanto pur non configurandosi particolari informazioni da introdurre nelle nomine ad incaricati che effettuino dei trattamenti con dispositivi mobili evoluti, può essere necessario integrare adeguatamente le istruzioni fornite in merito alla corretta realizzazione dei suddetti trattamenti.

Notificazione dei trattamenti

Tra i diversi adempimenti che occorre prendere in considerazione per garantire la piena *compliance* dei trattamenti effettuati, per l'ambito *mobile* occorre annoverare certamente la notificazione, obbligo previsto per i titolari qualora effettuino trattamenti specifici. In particolare una delle casistiche elencate dall'art. 37 e successivamente oggetto di chiarimento da parte dell'autorità Garante Privacy[18] può risultare particolarmente legato all'ambito *mobile*: si tratta di quanto indicato alla lettera a) comma 1 dell'art. 37 e si rivolge chiaramente all'impiego di strumenti per la georeferenziazione e utilizza una curiosa, quanto lungimirante definizione, parlando di "posizione geografica di persone od oggetti".
Infatti il legislatore pareva avere ben presente quello che oggi è di comune dominio, ovvero la diffusione di *device* in grado di fornire direttamente o indirettamente, le coordinate geografiche di una persona, tenendo anche in considerazione che la posizione di un ogget-

[17] Si veda, in particolare, il documento 00264/10/IT – WP169.
[18] Indicazioni del Garante Privacy sulla notificazione del 31 marzo 2004 e del 23 aprile 2004.

to che non si riferisse ad alcuno dei soggetti individuati all'art. 4, comma 1, lett. i), sarebbe del tutto irrilevante nell'ambito normativo di cui si tratta.

Tra gli ulteriori elementi, specifici dell'ambito *mobile*, che possono essere soggetti a notificazione, si evidenzia anche l'analisi dei profili degli utilizzatori assegnatari dei dispositivi (siano essi dipendenti, collaboratori o personale alle "dipendenze" di soggetti terzi) al fine di determinarne abitudini, scelte di consumo e/o per monitorare l'utilizzo dei servizi di comunicazione elettronica.

Gestione degli adempimenti formali da parte di soggetti terzi

A tali adempimenti formali si aggiunge poi il corretto indirizzamento del rispetto degli adempimenti Privacy da parte di eventuali *outsourcer*. Non di rado, le società affidano all'esterno la gestione di specifici servizi con particolare rilevanza nell'ambito specifico dei servizi di telecomunicazione, siano essi tradizionali ovvero annoverabili tra i c.d. VAS o Value Added Services.
La gestione di una flotta di auto, il tracking del personale o di mezzi che devono essere georeferenziati, il trattamento di dati personali dei dipendenti (conteggio delle chiamate personali, …) sono tutti trattamenti demandati in *outsourcing* che implicano l'esigenza di indurre il terzo di cui ci si avvale al rispetto della normativa applicabile, sia per quanto concerne gli adempimenti formali che per quanto riguarda le misure di sicurezza.

Pertanto l'attribuzione di tali trattamenti a soggetti esterni dovrebbe includere una valutazione dei seguenti elementi:

- integrazione negli aspetti contrattuali del rispetto di tutti gli adempimenti Privacy, non secondo una generica dicitura (insufficiente per evitare possibili contestazioni e *litigation*), ma entrando nel merito degli specifici elementi normativi applicabili. La catena virtuosa che dovrebbe consentire il controllo sui trattamenti dei dati e un adeguato livello di sicurezza può essere in tal senso viziata da aspetti non opportunamente indirizzati dati per scontato.
- Tra i punti da indirizzare nelle suddette parti contrattuali si evidenziano ulteriori elementi quali:
  - misure di sicurezza da adottare (spesso non è sufficiente il mero riferimento all'Allegato B del c.d. codice Privacy);
  - sessioni di verifica del rispetto delle disposizioni contrattuali;
  - relazione periodica sulle verifiche condotte in "auto-analisi" dal fornitore;
  - elenco degli amministratori di sistema, periodicamente aggiornato e comunque sempre disponibile - nella versione più aggiornata, a richiesta, in un brevissimo arco di tempo;
  - previsione di penali per il mancato rispetto delle disposizioni sopra menzionate;
- nomina a responsabile esterno, del soggetto esterno, in molti casi non effettivamente formalizzata con uno specifico atto.

Gli ulteriori ambiti normativi da tenere in considerazione

Oltre alla normativa Privacy, l'adozione di dispositivi mobili evoluti per la realizzazione di trattamenti di dati personali in ambito aziendale deve essere effettuata tenendo in considerazione ulteriori ambiti normativi.

Lo statuto dei lavoratori (legge 20 maggio 1970, n. 300)

Un secondo ambito normativo da prendere in considerazione, quando i trattamenti riguardano, direttamente o indirettamente, dati afferenti al personale aziendale, è sicuramente quello regolato dalla L. 300/1970 ovvero del cosiddetto "Statuto dei lavoratori". La diffusione dell'assegnazione in ambito aziendale per motivi lavorativi di telefoni mobili prima e dei dispositivi mobili evoluti poi, ha introdotto degli elementi di rischio già evidenziati in precedenza, relativi a trattamenti non conformi alle normative vigenti, quali, ad esempio, al controllo a distanza del lavoratore. L'analisi di tale aspetto richiede però una corretta contestualizzazione.
I dispositivi mobili evoluti sono infatti assegnati in ambito aziendale per poter sfruttare i

benefici evidenziati nei capitoli precedenti e per agevolare alcune esigenze operative (e.g. per facilitare le attività di reperibilità del personale permettendo una gestione da remoto, per fornire al lavoratore uno strumento che ne aumenti la produttività, …). Assodata la necessità di effettuare tali assegnazioni e le attività derivanti con i dispositivi mobili evoluti, è altresì possibile che si generino in ambito aziendale delle esigenze di analisi dei dati originati dall'utilizzo di tali dispositivi. Anche in tale caso, i trattamenti dei dati personali dei lavoratori correlati all'utilizzo di smartphone e tablet possono derivare da obiettivi:

- relativi agli aspetti gestionali/professionali, per tenere sotto controllo i costi aziendali;
- disciplinari, correlati al fatto che la diffusa attribuzione di dispositivi mobili evoluti, con l'elevato numero di servizi che questi possono garantire, può inevitabilmente determinare un aumento della frequenza degli abusi/degli utilizzi impropri degli stessi, determinando quindi la necessità di predisporre opportuni controlli (si pensi ad esempio alla verifica di un elevato utilizzo dei dispositivi per servizi di traffico telefonico/telematico non giustificati[19]);
- di conformità alla normativa cogente (si pensi ad un utilizzo dei dispositivi che integri una delle fattispecie di reato previste dal D.Lgs.231/2001).

Ovviamente tali trattamenti devono però garantire il corretto equilibrio tra le suddette esigenze delle società, la protezione dei dati personali e la tutela dei lavoratori. In tal senso, le peculiarità di tali dispositivi e degli utilizzi dei servizi rendono particolarmente complessa l'individuazione di tale punto di bilanciamento.

Tra queste peculiarità, già illustrate, sotto vari punti di vista, si evidenziano:

- le caratteristiche integrate di localizzazione e di miniaturizzazione delle antenne GPS, che hanno reso possibile la diffusione di strumenti di tracciamento della posizione dell'utente (utili in un ampio ventaglio di situazioni: settore autonoleggio, settore trasporto merci pericolose e quant'altro), che hanno rilevanza in materia giuslavoristica nel momento in cui l'utente viene interessato dal servizio in virtù della sua veste di lavoratore. Si tenga conto che non sempre le informazioni rilevate tracciano esplicitamente la posizione o il comportamento in tempo reale: è possibile, infatti, che la posizione venga rilevata in presenza di determinati indicatori oppure in determinate circostanze, ma che tali informazioni desunte consentano comunque di ricostruire gli spostamenti o i comportamenti del lavoratore.
- l'affermazione di un utilizzo "ibrido" (i.e. personale e professionale) di tali dispositivi[20]. Tale elemento rende ancora più critica la realizzazione di eventuali trattamenti che possono interessare dati personali che esulino dalla veste di lavoratore dell'interessato (si pensi ad esempio all'eventuale tracciamento del lavoratore fuori dai normali orari di servizio);
- l'attribuzione del dispositivo in qualità non di asset, bensì di benefit aziendale.

Per tutti questi motivi il Gruppo di Lavoro ritiene che, qualora siano determinate delle specifiche esigenze di trattamento dei dati personali dei lavoratori scaturite dall'utilizzo dei dispositivi mobili evoluti per fini aziendali, si debba procedere:

- individuando e indirizzando gli adempimenti formali;
- formalizzando le finalità e le modalità con cui i trattamenti dovrebbero essere effettuati, definite sulla base del corretto bilanciamento delle esigenze aziendali e della protezione dei dati dei lavoratori;
- condividendo formalmente, tali attività, con le rappresentanze sindacali.

Ovviamente fanno eccezione a quanto indicato quei trattamenti esplicitamente richiesti dalla normativa cogente.

[19] Con il termine "traffico" si intende, genericamente, l'attività legata all'uso del "mobile device".

[20] Tale aspetto è tra l'altro previsto anche da un provvedimento dell'Autorità Garante, espresso con le Linee Guida del 01/03/2007, sull'utilizzo degli strumenti di email e navigazione Internet, come presentato nei capitoli successivi.

Il D.Lgs. 231 (Decreto legislativo 8 giugno 2001, n. 231)

Un ulteriore ambito normativo da tenere in considerazione all'atto della realizzazione di trattamenti mediante i dispositivi mobili evoluti è quello, già citato, relativo al D.Lgs 231 per la responsabilità amministrativa di impresa. Tale normativa estende alle persone giuridiche la responsabilità per reati commessi in Italia ed all'estero da persone fisiche che operano per la società. Diversi interventi normativi hanno, nel corso degli ultimi anni, ampliato il novero dei reati alla commissione dei quali segue l'imputazione, in capo alla società, della responsabilità ex 231. La Convenzione di Budapest ha esteso tale normativa anche ai reati informatici ed a quelli commessi in violazione del disposto del TU in materia di Privacy[21].

Indubbiamente, seppure non sia introdotto il reato specifico di cui all'art. 167 del T.U. Privacy, l'inserimento dei c.d. reati informatici comporta che l'ente debba dotarsi di procedure interne specifiche volte a prevenire la commissione di reati attinenti gli apparecchi, le reti e i dati aziendali. La sicurezza informatica, quindi, analogamente a quanto già prescritto con il T.U. Privacy e l'introduzione delle misure di sicurezza, è positivizzata come un valore che le aziende devono assicurare sia ai fini della stessa tutela aziendale contro attacchi e abusi da parte di terzi sia come un valore economico e di mercato perché garantisce l'uso corretto e la fiducia dei clienti. L'ente, quindi, dovrà implementare tutte quelle "misure di carattere organizzativo" funzionali alla possibile esenzione da responsabilità amministrativa dell'ente, come previsto dall'art. 6 D.Lgs. n. 231/2001.

Al fine di non incorrere nelle sanzioni l'ente dovrà provare:

- che l'organo dirigente ha adottato e attuato un modello di organizzazione idoneo;
- che il compito di vigilare sul funzionamento e l'osservanza di detto modello e di curarne l'aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

L'art. 6 comma 2, indica poi le caratteristiche minime fondamentali cui il modello organizzativo deve rispondere, prescrivendo, in particolare:

- che esso "individui le attività nel cui ambito possono essere commessi reati";
- che preveda regole dirette a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire e individuare le modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- che siano previsti obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- che sia creato un sistema disciplinare (nel senso indicato in seguito, ossia riferito alla violazione delle regole contenute nel modello di prevenzione D.Lgs. n. 231/2001).

Quindi, per la prevenzione relativa ai reati informatici, dovrà essere attentamente formulata un'individuazione delle aree a rischio tra le quali, per quanto attiene anche l'oggetto di questo documento, i rischi connessi l'utilizzo di apparecchi *mobile*.

La prevenzione dei reati di cui all'art. 24-bis genera un impatto diretto su diversi settori aziendali, all'interno dei quali potrebbero svilupparsi le condizioni per la commissione di un delitto informatico, come conseguenza di comportamenti illeciti dei dipendenti che utilizzano gli strumenti e le tecnologie informatiche aziendali per svolgere il proprio lavoro.

In particolare basti pensare al concreto rischio di utilizzo delle tecnologie informatiche per carpire indebitamente informazioni al fine di perseguire un vantaggio economico per la propria azienda o per arrecare un danno a un'organizzazione "competitor".
Sarà necessario, quindi, sviluppare adeguate policy aziendali che ricomprendano in modo esplicito l'ambito dei reati informatici e individuino le sanzioni disciplinari a carico di coloro che violino in maniera intenzionale i sistemi di controllo o le indicazioni comportamentali fornite in materia.

[21] In realtà, nonostante il titolo accenni al TU privacy, le fattispecie penali indicate non annoverano l'art. 167 del D.Lgs 196/2003.

Il sistema di controllo per la prevenzione dei reati di criminalità informatica dovrà basarsi, in particolar modo, sui principi previsti dal TU Privacy anche per assicurare una corretta classificazione delle informazioni aziendali e di un'adeguata definizione dei differenti profili per il loro trattamento in accordo alle attività che su di esse vengono consentite con un'adeguata distinzione dei diversi profili operativi sui dati e sulle informazioni.
Ai fini, poi, del controllo e del monitoraggio delle attività illecite sarà necessario provvedere alla tracciabilità degli accessi e delle attività svolte sui sistemi informatici che supportano i processi esposti a rischio.

Tale attività può rivelarsi problematica visto l'utilizzo, da parte dei soggetti apicali, di strumenti aziendali quali tablet e smarthphone (che, quindi, sfuggono a un controllo diretto sia sul supporto che al momento nel quale esso viene utilizzato) che possono diventare lo strumento attraverso il quale perpetrare un crimine informatico.
Rischio elevato se si pensa all'ipotetico caso di un dipendente che si connetta abusivamente, con il tablet aziendale che utilizza per fini lavorativi, ad una rete wi-fi di terzi. Parte della giurisprudenza ritiene configurabile il reato di accesso abusivo a sistema informatico anche l'accesso ad un sistema non protetto da password (e, in particolar modo la permanenza contro lo ius excludendi del titolare della rete): quindi, anche una rete wi-fi non protetta.
Sarà ritenuta responsabile, quindi, la società per l'accesso abusivo a sistema informatico commesso dal proprio dipendente?

Astrattamente ci sono tutti gli elementi che configurano tale ipotesi ex art. 24 bis Legge 231/2001: l'ente, infatti, è responsabile per i reati commessi nel suo interesse o a suo vantaggio e anche il semplice sfruttamento di una rete altrui può essere ritenuto un vantaggio, seppur minimo, in capo alla società.

CASE STUDY - Georeferenziazione

Relativamente agli adempimenti formali evidenziati in precedenza, si ritiene che un case study di particolare rilevanza nell'ambito del mobile, sia quello relativo alla georeferenziazione, riferendosi con tale termine al trattamento di dati correlati al posizionamento geografico di un dispositivo (e quindi dell'eventuale persona associata). La normativa di riferimento individua specifici adempimenti nella realizzazione del suddetto trattamento di dati, ovvero:

- l'accordo sindacale, puntualmente analizzato nei paragrafi correlati allo statuto del lavoratore;
- la notificazione: i provvedimenti adottati dall'Autorità Garante Privacy proprio per fare chiarezza sulle situazioni ancora soggette all'adempimento della notificazione, non escludono questa necessità, ma anzi la ribadiscono, tanto che nei provvedimenti più recenti, specificamente riguardanti applicazioni di georeferenziazione, di persone e di mezzi, il Garante coglie spunto per indicare fra gli adempimenti richiesti per un legittimo trattamento dei dati, ad opera di un servizio di georeferenziazione, l'essenzialità di quest' adempimento;
- la verifica preliminare: i trattamenti in oggetto rientrano a buon titolo fra quelli che presentano rischi specifici ex articolo 17, a termini del quale: il trattamento che presenta rischi specifici per i diritti e libertà fondamentali nonché per la dignità dell'interessato in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

Pertanto, puntuali misure ed accorgimenti sono prescritti dal Garante, nell'ambito di una verifica preliminare. Questa verifica consiste nella sottoposizione all'Autorità, da parte del titolare del trattamento, di un dettagliato documento descrittivo dell'attività che si intende condurre. Il documento dovrà contenere precise indicazioni, sia per quel che riguarda il data flow, sia sotto i diversi aspetti che garantiscono la tutela dell'interessato, tanto in termini di informative e raccolta di consapevole consenso, quanto in termini di misure di sicurezza (sempre tenendo conto del quadro normativo d'insieme).

Altre considerazioni

In occasione dei procedimenti di verifica preliminare (ma anche nell'esercizio della propria attività di controllo), in relazione ai trattamenti effettuati mediante tali sistemi nell'ambito dell'esecuzione del rapporto di lavoro, per soddisfare esigenze organizzative e produttive ovvero per la sicurezza sul lavoro, il Garante ha adottato nel tempo alcune importanti decisioni (cfr. Provv.ti 18 febbraio 2010, in www.garanteprivacy.it, doc. web n. 1703103; 7 ottobre 2010, doc. web n. 1763071; 7 luglio 2011, docc. web n. 1828371 e 1828354). Per la sua portata generale, spicca il provvedimento "Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro" datato 4 ottobre 2011. In esso, oltre ad evincersi gli adempimenti di cui sopra, viene fatto un esplicito richiamo all'istituto del bilanciamento degli interessi, nonchè ai principi fondamentali che devono guidare l'adozione di applicazioni (in senso molto ampio) di localizzazione. La possibilità di individuare, in un dato momento, la posizione dei lavoratori, mediante sistemi di localizzazione, può rivelarsi utile per soddisfare esigenze organizzative e produttive ovvero per la sicurezza sul lavoro. Queste finalità possono ricorrere, ad esempio, per soddisfare esigenze logistiche, per elaborare rapporti di guida allo scopo di commisurare il tempo di lavoro del conducente, ovvero per commisurare i costi da imputare alla clientela, nonché per assicurare una più efficiente gestione e manutenzione di un parco veicoli, con effetti vantaggiosi anche sulla sicurezza sul lavoro e per la sicurezza della collettività. Se vengono adottate le garanzie previste dallo Statuto dei lavoratori, i datori di lavoro privati e gli enti pubblici economici possono effettuare lecitamente il trattamento dei dati personali (diversi da quelli sensibili), relativi all'ubicazione dei propri dipendenti, per soddisfare le esigenze sopra esposte (oltre che sulla base di uno degli altri presupposti di cui all'art. 24 del Codice), anche in assenza del consenso degli interessati, per effetto di un provvedimento (che può avere anche portata generale come quello del 4 ottobre 2011) che, in applicazione della disciplina sul c.d. bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice), individui un legittimo interesse al trattamento di tale tipologia di dati. Il Garante richiede poi al titolare del trattamento una valutazione rigorosa dei dati coinvolti nel trattamento de quo, guidata dal principio di pertinenza e non eccedenza (per far sì che vengano trattati solamente i dati strettamente necessari al perseguimento delle predette finalità). Infine, l'attenzione viene focalizzata sulla necessità di individuare il fornitore del servizio come responsabile esterno del trattamento (ex articolo 29), impartendo le necessarie istruzioni in ordine all'utilizzo legittimo dei dati raccolti e determinando, altresì, modalità e tempi della loro, eventuale, conservazione.

Misure minime di sicurezza

Premessa

Preliminarmente all'analisi puntuale delle misure di sicurezza correlate ai trattamenti di dati personali effettuati mediante dispositivi mobili evoluti, è necessario puntualizzare un aspetto chiave in merito alla loro classificazione ed al loro carattere di "obbligatorietà". È infatti uso comune la classificazione delle misure di sicurezza da adottare a protezione dei dati personali trattati in due tipologie principali:

- le misure minime;
- le misure idonee.

Questa suddivisione ha visto l'erronea sovrapposizione del concetto di misure obbligatorie alle sole misure minime, relegando al livello di "facoltative" quelle idonee. In realtà il Gruppo di Lavoro ritiene che, per un corretto approccio alla tematica, ci si debba riferire non solo agli Artt. 31 e 33 del Codice Privacy, ma anche all'art.154. Se i primi due articoli forniscono la definizione degli obblighi di sicurezza e dei livelli minimi di sicurezza, quest'ultimo articolo attribuisce all'Autorità Garante per la Privacy la facoltà di prescrivere in taluni casi e di "curare la conoscenza" in altri specifiche adempimenti, determinando quindi un ulteriore elemento di cogenza normativa. In sintesi pertanto, secondo l'attuale contesto normativo è possibile identificare tre tipologie di misure di sicurezza, ovvero:

Figura 5
Le tre tipologie di misure di sicurezza

Pertanto le analisi delle misure di sicurezza di seguito presentate saranno strutturate in conformità a tale modello.

Nota bene:
Potrebbero altresì intendersi come indicazioni comunque correlate con l'attività di gestione della sicurezza aziendale, anche i divieti imposti ex art. 154, comma 1, lett. d); questi divieti, in taluni casi sono espliciti e indicano quali attività non devono essere poste in essere, di fatto rivelandosi come vere e proprie misure di sicurezza da porre in essere, ad esempio:

- il divieto di lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- il divieto di riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- il divieto di procedere con la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- il divieto di procedere all'analisi occulta dei computer portatili affidati in uso.

Misure minime di sicurezza in ambito *mobile*

Per quanto concerne le misure minime di sicurezza, introdotte come indicato in precedenza dall'articolo 34 del Codice e meglio specificate nel Disciplinare Tecnico (Allegato B), è possibile rilevare che nel contesto dei dispositivi *mobile* sono applicabili tutte le prescrizioni

riferibili ai trattamenti effettuati attraverso strumenti elettronici. Tuttavia, gli aspetti peculiari (tanto tecnologici quanto di utilizzo) dei suddetti dispositivi determinano la necessità che tali misure minime siano opportunamente ripensate ed implementate, al fine di proteggere opportunamente i dati personali trattati dai rischi illustrati in precedenza. Tale ripensamento è necessario al fine non solo di evitare che un'erronea o una mancata attuazione delle misure minime per il contesto *mobile* possa prefigurare una sanzione penale o amministrativa, ma altresì di incorrere in ben più gravi incidenti di sicurezza relativi alla perdita dei parametri di sicurezza (riservatezza, integrità e disponibilità) dei dati.

Come per tutti gli ambiti generali, anche per lo specifico ambito *mobile*, tali misure minime sono riconducibili alle seguenti tipologie:

a) adozione di meccanismi di autenticazione informatica;
b) gestione delle credenziali di autenticazione;
c) adozione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) aggiornamento periodico dei programmi per elaboratore per prevenire vulnerabilità e difetti;
g) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
h) tenuta di un aggiornato documento programmatico sulla sicurezza[22];[1]
i) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Date le peculiarità dei dispositivi in questione tali misure saranno di seguito analizzate in una chiave di lettura più specifica, affinché esse possano risultare coerenti con le nuove sfide aperte dal mondo *mobile*.

a) Adozione di meccanismi di autenticazione informatica

L'ambito delle misure introdotto dal Disciplinare Tecnico (Allegato B) evidenzia la necessità che l'accesso ai dati per il loro trattamento attraverso strumenti elettronici sia effettuato a fronte del "superamento di una procedura di autenticazione". Negli ambiti tecnologici più "tradizionali", tali meccanismi verificano l'identità dell'utente relativamente alle seguenti tipologie di accessi:

- accesso alla macchina (PC, desktop, laptop…), spesso coincidente con gli accessi al dominio di rete aziendale;
- accesso a servizi/sistemi IT, mediante un ulteriore livello di autenticazione, il quale può essere centralizzato (e.g. Single Sign On, SSO) oppure correlato ad ogni singolo servizio/sistema.

Più difficilmente invece il controllo avviene a livello di singolo elemento informativo (e.g. file o cartella di rete) e/o a livello di supporto correlato. Tale aspetto calato nell'ambito *mobile* deve essere invece necessariamente contestualizzato relativamente ai seguenti aspetti:

- accesso al dispositivo: in analogia a quanto esistente per qualsiasi dispositivo elettronico, anche per accedere alle funzionalità del dispositivo mobile è necessario che sia previsto un meccanismo di autenticazione che determini la reale identità dell'utente che sta cercando di accedere. Tale elemento è in alcuni casi confuso però con l'attivazione del PIN della scheda SIM (si veda il punto successivo), che permette l'accesso ad alcuni servizi (generalmente quelli telefonici/ telematici). Al fine di soddisfare pienamente tale la misura minima, è quindi necessario che, anche qualora sprovvisti di SIM telefonica, l'accesso al dispositivo sia opportunamente regolamentato, mediante un meccanismo basato almeno sull'utilizzo delle credenziali (codice identificativo e componente segre-

[22] Per quanto riguarda i recenti aggiornamenti normativi promossi con il D.L.05/2012 (c.d. decreto "Semplificazioni"), si rimanda alla nota introduttiva del paragrafo per una breve analisi della situazione evolutiva.

ta…). Tale elemento è maggiormente evidente nei tablet, ma potrebbe essere trascurato negli smartphone;

- accesso alla scheda SIM: il processo di autenticazione sulla scheda SIM offerto dal dispositivo, permette generalmente l'attivazione dei servizi telefonici e telematici (connessioni…) associati all'utenza ed in alcuni casi del dispositivo. Tale aspetto, se non opportunamente indirizzato, può determinare delle criticità di sicurezza sia dirette che indirette. A titolo di esempio, una criticità diretta della mancata applicazione di meccanismi di accesso alla SIM, quella correlata all'accesso non autorizzato ai contatti (qualificabili come dati personali a tutti gli effetti e senza tenere eventualmente conto del valore che essi possono avere a livello aziendale), mentre le criticità indirette possono essere correlate al fatto che il possesso della SIM è associato, in alcuni processi di autenticazione, all'identità dell'assegnatario e pertanto utilizzato come elemento identificante per l'accesso a molti servizi (e.g. si pensi ad esempio ad un servizio di reset password offerto mediante Helpdesk telefonico che identifichi l'utente sulla base del numero chiamante), elemento che potrebbe quindi determinare una successiva perdita di protezione dei dati personali trattati in azienda;
- accesso ai supporti di memorizzazione: l'elevata capacità di memorizzazione degli attuali dispositivi è garantita sia da supporti presenti nel dispositivo stesso (*hard disk* interno) sia da supporti esterni, che sono caratterizzati da dimensioni sempre minori. Dato l'alto valore potenziale delle informazioni in essi contenute, è opportuno che siano presi in considerazione la possibilità, in aggiunta ad eventuali misure di cifratura, di meccanismi di autenticazione anche sui supporti stessi;
- accesso a livello di singolo servizio IT / Sistema IT: così come già esistente per i precedenti dispositivi mobili (laptop…) anche per i dispositivi mobili evoluti è di particolare importanza la gestione degli accessi ai sistemi e ai servizi accessibili dal dispositivo. Tenendo inoltre in considerazione tutti gli attuali trend di utilizzo ed in particolare l'affermarsi degli approcci BYOD, evidenziati in precedenza, tale livello del controllo accessi è da considerare ancora più rilevante. La perdita della governance diretta sui dispositivi che tali politiche possono introdurre, determina, infatti, che sia necessario rafforzare il livello di controllo accessi correlato agli accessi ai dati personali direttamente sui servizi ed i sistemi IT.

Infine in caso di furto o perdita di dispositivo *mobile*, l'accesso ai dati su di esso contenuti potrebbe avvenire tramite collegamento (es. porta USB) a PC. Anche in questo caso potrebbe essere opportuno prevedere qualche meccanismo di autenticazione (utilizzo di credenziali di autenticazione) che permetta di identificare il soggetto che sta cercando di accedere ai dati in questione.

Tutti gli aspetti precedenti devono essere ovviamente indirizzati in maniera integrata con l'adozione la definizione di parametri dei diversi dispositivi che prevedano delle *session time-out* che blocchino il telefono automaticamente, richiedendo l'autenticazione (ai diversi livelli precedenti), a fronte di un predeterminato tempo di assenza di interazione con il dispositivo. Tale tempistica di attivazione deve essere ovviamente il giusto compromesso (determinato dall'analisi dei rischi) tra operatività e sicurezza.

Pertanto, al fine di essere pienamente conformi alle indicazioni normative e di garantire un opportuno livello di protezione dei dati trattati è necessario che i meccanismi di controllo degli accessi per l'autenticazione siano applicati a tutti i livelli tecnologici necessari.

L'attivazione di tali meccanismi deve avvenire all'accensione dei dispositivi, ai tentativi di accesso alle diverse componenti degli stessi e a fronte del rientro da situazioni di blocco dovute all'attivazione di meccanismi di session time-out che devono essere necessariamente integrati con il controllo accessi.

b) Gestione delle credenziali di autenticazione

Per quanto concerne i restanti requisiti di autenticazione, specificati nei punti del Disciplinare Tecnico (All.B) da 2. a 11., si evidenzia come, nell'ambito dei dispositivi mobili evoluti, fatta eccezione per il livello di autenticazione ai servizi ed ai sistemi IT (per i quali

si possono applicare le tradizionali considerazioni) essi siano solo parzialmente applicabili e comunque debbano essere opportunamente re-interpretati.

In primo luogo per alcune tipologie di tali dispositivi (principalmente per gli smartphone), l'autenticazione è effettuata generalmente solamente attraverso l'inserimento di una componente segreta, senza però l'associazione di un codice per l'identificazione[23] (ID). Tale considerazione è generalmente correlata al fatto che tali dispositivi sono assegnati in maniera univoca ad un unico utente. Per altri invece (e.g. per i tablet) i suddetti requisiti normativi continuano ad avere valore.

Relativamente all'elemento di verifica per l'autenticazione, nell'ambito dei dispositivi mobili evoluti, la componente verificata consiste generalmente in qualcosa che l'utente del dispositivo conosce, piuttosto che qualcosa che l'utente possiede o che lo caratterizza. Tale aspetto è determinato principalmente dalla comodità di trasporto e di complessità di integrazione dei dispositivi in infrastrutture di autenticazione più complesse (quali ad esempio meccanismi di strong authentication). Ciononostante, qualora ritenuto rilevante (soprattutto sulla base delle indicazioni delle attività di analisi dei rischi), sono disponibili delle soluzioni che rendono possibile l'adozione anche dei due ulteriori elementi di autenticazione, così come già introdotto in tempi successivi in maniera integrata per i precedenti dispositivi portatili[24].

Anche in relazione alle caratteristiche di lunghezza, periodicità di scadenza e modalità di cambio della componente segreta, introdotti dal punto 5. del Disciplinare Tecnico (all.B), i requisiti debbono essere ripresi attentamente in considerazione. In particolare:

- la componente segreta per alcuni livelli di accesso (SIM e supporti di memoria) è generalmente costituita da un PIN che ha quindi una lunghezza tecnicamente limitata;
- la modifica al primo utilizzo rimane comunque consigliata;
- la periodicità di cambio dovrebbe invece rispettare pienamente il requisito specificato, anche se essa può per alcune tipologie di dispositivi solamente essere implementata demandando tale gestione alla gestione dell'utente stesso, senza una gestione automatizzata centralizzata che possa forzare queste policy.

Anche per tale aspetto, qualora sia evidenziata la necessità nell'ambito dell'analisi dei rischi, è possibile avvalersi di soluzioni evolute presenti sul mercato.

Gli aspetti illustrati in precedenza di utilizzo della sola componente segreta e della sua modifica periodica, determinano una complessità nella soddisfazione del requisito del punto 10. del Disciplinare Tecnico (all.B): tale punto introduce infatti la necessità, nel caso di utilizzo della sola password, di prevedere l'adozione di misure organizzative e procedurali affinché la stessa sia acquisita, conservata e successivamente recuperata per l'accesso ai dati in caso di prolungata assenza o impedimento dell'incaricato. Tali misure devono prevedere tra l'altro l'identificazione di incaricati alla custodia di tali componenti.

Infine particolare rilevanza per il contesto mobile assumono i requisiti del punto 4. e 9. relativamente alla necessità di predisposizione per gli incaricati di istruzioni che prescrivano la necessaria cura per la custodia della password e la necessità di non lasciare incustodito e accessibile lo strumento durante un trattamento.
Quest'ultimo punto risulta particolarmente critico in virtù delle maggiori criticità in termini di protezione dei dati nei dispositivi mobili, sia relativamente alla massima cautela affinché i dispositivi non siano persi o rubati ed altresì affinché i dati non siano accessibili a soggetti terzi durante la temporanea sessione di trattamento (ad esempio implementando misure di session time-out).

[23] Rif. Artt. 2, 3, 6, 7 e 8 del Disciplinare Tecnico.
[24] Si pensi ad esempio all'attuale diffusione dei dispositivi integrati di autenticazione biometrica per laptop.

Pertanto, le caratteristiche dei meccanismi di autenticazione e delle credenziali di accesso ai dati per i dispositivi mobili evoluti devono essere attentamente analizzate ed implementate al fine di cercare di soddisfare pienamente i requisiti introdotti dal Disciplinare Tecnico.

c) Adozione di un sistema di autorizzazione

In analogia a quanto detto per i punti precedenti, anche per i requisiti introdotti dai punti 12., 13. e 14. del Disciplinare Tecnico è possibile identificare che:

- per quanto concerne gli accessi ai servizi ed ai sistemi IT, i requisiti si applicano come per gli ambiti tecnologici tradizionali. I profili di autorizzazione sono configurati a livello applicativo e centralizzato al fine di consentire l'accesso ai soli dati necessari. Sarà necessario prevedere una classificazione degli applicativi e dei dati accessibili tramite dispositivi mobili e le relative autorizzazioni all'accesso. Periodicamente deve essere verificata l'adeguatezza del profilo di accesso e delle relative permission sui dati esportabili sui dispositivi mobili;
- per i restanti livelli di accesso, per alcune tipologie di dispositivi (soprattutto per gli smartphone), gli aspetti di profili autorizzativi e di loro gestione, sono da ritenere applicabili solo mediante l'adozione di specifiche soluzioni;

Pertanto, gli aspetti di controllo dei profili autorizzativi per gli accessi ai dati sono implementabili per l'accesso ai servizi ed ai sistemi IT, mentre lo sono solo per alcune tipologie di dispositivi per le altre tipologie di accesso.

d) Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici

Il Disciplinare Tecnico (All.B) al punto 15. introduce il requisito di aggiornamento periodico (almeno annuale) per l'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione. Tale requisito risulta essere invariante per l'ambito mobile rispetto i processi tecnologici ed organizzativi tradizionali. Ciononostante potrebbe essere opportuno prendere in considerazione se gli eventuali profili autorizzativi e gli ambiti di trattamento effettuati attraverso accessi da questi dispositivi debbano essere analizzati e tracciati in maniera puntuale.

e) Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici

Il Disciplinare Tecnico (All.B) al punto 16. introduce il requisito di aggiornamento delle soluzioni adottate per la protezione dei sistemi, con particolare attenzione da malware.

Pur essendo in netta evoluzione, tale requisito in ambito *mobile* risulta essere un elemento di difficile implementazione e gestione, soprattutto per quegli ambiti dove il parco tecnologico dei dispositivi è piuttosto differenziato o addirittura non è definito a priori (e.g. in un contesto aziendali che applichi le strategie di BYOD).

Tale criticità è determinata dal fatto che le attuali soluzioni tecnologiche hanno generalmente validità solo per specifiche piattaforme/specifici S.O. con peculiarità a volte anche significative.

Sul sito Internet della presente iniziativa del Gruppo di Lavoro[25], vengono riportate le caratteristiche dei principali prodotti presenti sul mercato che garantiscono protezione per i dispositivi mobili da virus, malware, violazione dei dati, applicazioni dannose.
Particolarmente rilevanti risultano pertanto tutti gli aspetti di governo di tali soluzioni, dalla loro scelta (quali soluzioni sono più adatte al mio contesto tecnologico), della loro implementazione e del loro periodico aggiornamento, in conformità ai requisiti del Disciplinare Tecnico (All.B) ed al fine di proteggere efficacemente i dati.

[25] http://privacycloudmobile.clusit.it/pages/Download.html.

A supporto dell'attuazione di un efficace attuazione dei suddetti aspetti, è consigliabile che la gestione dei dispositivi, sia realizzata mediante l'adozione di piattaforme di governo degli stessi, quali le soluzioni di MDM e MDA, illustrate successivamente nel contesto delle misure idonee.

La protezione dei dati personali contro il rischio di intrusione e dell'azione di malware risulta particolarmente complessa in ambito mobile a causa della varietà dei dispositivi e delle soluzioni correlate. Pertanto l'individuazione, l'adozione e la gestione di tali situazioni dovrebbe essere attuata mediante approcci strutturati. Le soluzioni individuate dovrebbero essere poi successivamente governate mediante opportuni sistemi MDM/MDA.

f) Aggiornamento periodico dei programmi per elaboratore per prevenire vulnerabilità e difetti

Così come per le soluzioni anti-malware, anche l'attuazione della gestione delle patch di sistema operativo e dei programmi software introdotta dal punto 17. del Disciplinare Tecnico, in ambito mobile può risultare particolarmente complessa.
Seppure l'aspetto sia presente anche nei contesti tecnologici tradizionali, come illustrato in precedenza la possibile numerosità elevata del portafoglio tecnologico dei dispositivi mobile in ambito aziendale può determinare la necessità di governare diverse fonti informative dei produttori di dispositivi, di S.O., di programmi... Senza contare che, come nel caso del già citato approccio BYOD, tali aspetti possono anche non essere sotto il diretto governo delle funzioni aziendali.

In tale caso, al fine di garantire la piena conformità ai riferimenti normativi e soprattutto un'efficace protezione dei dati trattati, è consigliabile adottare un set limitato di soluzioni tecnologiche, governandole quindi con soluzioni strutturate ed integrate (e.g. MDM e MDA), già indicate al punto precedente.

g) Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi

Come illustrato nella descrizione del contesto tecnologico complessivo iniziale e nell'analisi di misure di sicurezza precedenti, la piena conformità al punto 18. del Disciplinare Tecnico (All.B) comporta che le istruzioni organizzative e tecniche prendano in considerazione il salvataggio dei dati, ovunque essi si collochino nel contesto dei dispositivi mobile.

In maniera invariante rispetto ai processi di gestione tecnologica tradizionali, anche per l'ambito mobile è necessario che siano

- definite delle misure che determinino le soluzioni tecniche di salvataggio dei dati (quali elementi sono soggetti a salvataggio, periodicità, infrastrutture di supporto…), prendendo in considerazione tutti gli elementi tecnologici (dispositivi, schede di memoria di supporto, elementi centralizzati dell'infrastruttura…);
- indicate quali sono le responsabilità correlate degli utenti (e.g. quelle di non conservare dati sui supporti mobili dei dispositivi o sui supporti interni dei dispositivi…).

Come illustrato relativamente agli aspetti di rischio però, in ambito mobile non è possibile ridursi unicamente a considerare il salvataggio dei dati su dispositivo, ma è altresì necessario tenere in considerazione quegli aspetti di configurazione presenti sugli elementi infrastrutturali centralizzati della piattaforma mobile aziendale.
La perdita di tali informazioni, seppur non direttamente correlata alla perdita dei dati e delle informazioni trattate, può determinare una sospensione anche non indifferente nell'effettuazione dei trattamenti (si prenda in considerazione in tal senso il già citato caso di indisponibilità dei servizi subito da RIM durante il 2011).

L'adozione di misure di salvataggio deve comportare la puntuale definizione dei diversi ruoli e responsabilità, ivi incluse quelle di eventuali soggetti terzi che gestiscano in outsourcing gli elementi infrastrutturali centralizzati dei servizi mobile.

h) Tenuta di un aggiornato documento programmatico sulla sicurezza

ATTENZIONE:

Con l'introduzione degli aspetti normativi del D.L.05/2012 (c.d. decreto "semplificazioni") tale misura, fino alla completa approvazione del D.L., assume la connotazione di misura idonea. Tuttavia, le prime indicazioni derivanti dal nuovo regolamento comunitario in tema Privacy sembrano voler riaffermare la necessita' di tale documento, ai fini di programmare misure adeguate ai rischi (Art.27 nuova direttiva), seppure con una denominazione e delle finalità leggermente modificate. Inoltre il Gruppo di Lavoro ritiene che tutte le attività "propedeutiche" alla redazione del DPS – censimento dei trattamenti, analisi dei rischi- continuano ad avere un carattere obbligatorio (il censimento essendo anche misura minima): pertanto a prescindere dalla specifica formalizzazione del documento, tutte le attività di analisi correlate devono essere ritenute necessarie e obbligatorie.

Anche per quanto riguarda la redazione del Documento Programmatico sulla Sicurezza (DPS), l'introduzione di trattamenti effettuati tramite dispositivi *mobile,* richiede particolari elementi di adeguamento. Al fine di monitorare la corretta protezione dei dati personali trattati attraverso tali dispositivi, si ritiene che sia rilevante integrare opportunamente:

- il censimento dei trattamenti, tracciando quelli fatti tramite tali dispositivi;
- l'analisi dei rischi, arricchendola di quei rischi specifici introdotti dall'utilizzo di tali dispositivi;
- il tracciamento delle specifiche misure di protezione dei dati personali adottate per l'ambito mobile.

La predisposizione del DPS dovrebbe pertanto prevedere esplicite considerazioni in merito ai trattamenti effettuati mediante i dispositivi mobili evoluti adottati in ambito aziendale.

i) Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari

Il Disciplinare Tecnico (All.B) al punto 24. introduce il requisito di tecniche di cifratura per i trattamenti specificati. Questo implica dover implementare:

una connessione protetta del canale per il trasferimento di tali dati anche da/verso i dispositivi mobili. È necessario quindi identificare protocolli e modalità di comunicazione dei dati e renderli sicuri (e.g. nessun trasferimento di dati in FTP verso sistemi centralizzati, servizi in cloud…)

la cifratura dei dati sull'hard disk interno del dispositivo o dei supporti removibili di memoria.

Il trattamento di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati tramite dispositivi mobili introduce la necessità di dover prendere in considerazione i canali di comunicazione utilizzati dal dispositivo, al fine di renderli sicuri e di adottare misure di cifratura per i diversi supporti (Hard disk, SD…) che contengono i dati sui dispositivi.

Misure obbligatorie di sicurezza

Come illustrato in precedenza, oltre alle misure minime, esiste un ulteriore insieme di requisiti cogenti, correlato ai vari provvedimenti (generali o per specifici soggetti) che l'Autorità Garante per la Privacy ha emanato. Tali integrazioni normative si differenziano, generalmente, sia per tipologia di dati trattati che per perimetro di applicabilità.

Ovviamente i provvedimenti applicabili in ambito *mobile* sono numerosi e prevedono diverse misure di sicurezza: di seguito riportiamo quelli che il Gruppo di Lavoro ritiene particolarmente rilevanti in relazione all'introduzione di dispositivi mobili all'interno dell'ambito aziendale.

Il Provvedimento Garante Privacy del 27 novembre 2008 (Amministratori di sistema)

Il provvedimento in questione e le sue successive integrazioni prescrive alle aziende, sia private che pubbliche, una serie di misure di natura organizzativa, procedurale e tecnica correlate al ruolo degli amministratori di sistema (intendendo come tali tutti gli addetti IT che realizzano attività quali la gestione sistemistica, la gestione dei database, l'amministrazione degli elementi di networking,…)

In relazione alle prescrizioni di tipo organizzativo e procedurale si evidenzia quanto segue:

- **Identificazione degli amministratori di sistema e predisposizione dell'elenco correlato**
  L'identificazione e la predisposizione del loro elenco dovrebbe includere esplicitamente anche coloro che gestiscono l'infrastruttura di tali dispositivi. Più in dettaglio, quindi, dovrebbero essere considerati in ambito non soltanto coloro che effettuano attività manutentive (da remoto o in locale) sui dispositivi, ma anche tutti coloro che si occupano degli elementi centralizzati: ad esempio in tale elenco dovrebbero essere inclusi anche tutti coloro che effettuano attività di gestione sul BES della piattaforma BlackBerry. Inoltre in conformità a quanto specificato ulteriormente dal provvedimento, coloro che amministrano tali dispositivi, potendo potenzialmente venire in contatto con dati personali riconducibili al personale aziendale (e.g. dati di navigazione, dati prodotti per finalità non lavorative…), dovrebbero essere ulteriormente inclusi nella lista creata ad hoc per gli amministratori di sistema che gestiscono sistemi con dati personali di tali interessati. Tale lista deve essere prodotta e pubblicata internamente secondo i canali ritenuti più opportuni (intranet, bacheca aziendale, comunicazione puntuale…).
- **Designazione individuale**
  La designazione individuale dei soggetti che effettuano attività di amministrazione dei suddetti dispositivi dovrebbe essere inclusiva anche di una specifica indicazione di operatività sui dispositivi mobili evoluti, in modo che anche gli amministratori stessi siano resi consci della potenziale criticità dei dati trattati su questi dispositivi.
- **Servizi in outsourcing**
  Come evidenziato in precedenza, nell'ambito di applicazione delle prescrizioni del provvedimento devono essere necessariamente inclusi anche gli amministratori di sistema dei soggetti terzi a cui siano demandate attività di outsourcing, con particolare attenzione per quei soggetti che realizzano attività di gestione degli elementi centralizzati delle piattaforme di tali dispositivi (e.g. infrastruttura BES). Ciò significa che, ai fini della normativa attuale, è necessario che sia richiesta a tali soggetti una predisposizione dell'elenco del loro personale che operi in qualità di amministratore di sistema per la società.
- **Verifica dell'attività**
  Relativamente alle verifiche, si evidenzia che anche il contesto tecnologico dei dispositivi mobili evoluti dovrà essere incluso nella revisione periodica (annuale) delle attività realizzate dagli amministratori di sistema.

In merito invece alle prescrizioni di natura tecnologica, che consistono nella registrazione e nella successiva conservazione dei log di accesso ai sistemi contenenti dati personali da parte degli amministratori di sistema, il Gruppo di Lavoro evidenzia quanto segue:

- l'adozione delle misure di tracciamento dovrebbe riguardare sia l'accesso ai dispositivi che agli elementi centralizzati. Tale aspetto però può determinare delle particolari criticità nel caso di gestione fornita da outsourcer IT: in tal caso gli aspetti di tracciamento dovrebbero essere gestiti mediante opportuni aspetti contrattuali e verificati periodicamente;
- l'indirizzamento di tali aspetti potrebbe creare delle complicazioni nel caso in cui tali soggetti terzi siano società operanti all'estero e non direttamente interessate dalla normativa Privacy italiana[26];
- gli aspetti indirizzati verso tali soggetti terzi dovrebbero tenere in considerazione anche aspetti correlati alla successiva gestione di tali log, quali il periodo di conservazione (almeno 6 mesi), le misure di protezione correlate (cifratura dei log), le modalità di accesso a tali log (motivazioni, i soggetti autorizzati …).

Più in generale, l'introduzione di tali dispositivi rende necessarie opportune integrazioni delle normali attività di gestione effettuate dalla società, determinando un allargamento del perimetro di gestione in merito a:

- nuovi sistemi in ambito;
- nuove piattaforme di interfaccia;
- nuovi soggetti preposti alla gestione;
- nuove misure di protezione…

Le linee guida Garante Privacy del 01 marzo 2007 (Gestione della email e della navigazione Internet)

Le linee guida in oggetto riguardano l'utilizzo degli strumenti informatici di posta elettronica e navigazione Internet sul luogo di lavoro e prevede, da un lato, un divieto generalizzato per le aziende di effettuare controlli su tali servizi in modo massiccio e permanente, dall'altro l'obbligo di informare i dipendenti e rendere per loro trasparente le modalità con cui utilizzarli, nonché le varie misure e modalità di controllo, in caso di utilizzo anomalo dei suddetti strumenti.

In particolare, l'azienda dovrà fornire preventivamente ai dipendenti un'informativa (prevista dall'articolo 13 del Codice della Privacy) chiara e particolareggiata, relativa ai trattamenti di dati che possono riguardarli e adottare un disciplinare/codice interno (una sorta di "Codice etico") nel quale siano chiaramente indicate le modalità di utilizzo degli strumenti messi a disposizione del dipendente (le regole per l'uso di Internet e della posta elettronica), nonché la possibilità di controlli da parte dell'azienda.

Il crescente e diffuso utilizzo di dispositivi mobili quali smartphone e tablet, che consentono la lettura di email e la navigazione Internet, quasi sempre in modalità promiscua, rende necessaria l'estensione del provvedimento in discussione e la rivalutazione delle disposizioni vigenti alla luce dei nuovi rischi introdotti, in termini di:

- aggiornamento della documentazione formale di utilizzo di tali dispositivi (disclaimer, informative, consensi…);
- aggiornamento del codice "etico" che vincoli tali attività sia in termini di trasparenza sui controlli a cui tali dispositivi potrebbero essere esposti in caso di anomalie nell'utilizzo degli stessi;
- estensione delle misure tecniche di protezione perimetrale (firewalling…) anche all'ambito *mobile;*
- definizione della regolamentazione dell'utilizzo del dispositivo per finalità personali (chiamate, utilizzo della connettività, utilizzo delle caratteristiche di memorizzazione…);
- definizione delle modalità di verifica degli utilizzi scorretti di tali dispositivi e delle successive attività di richiamo e di sanzionamento disciplinare.

Il Provvedimento Garante Privacy del 13 ottobre 2008 (RAAE)

- Il provvedimento in oggetto riguarda le modalità di reimpiego e dismissione delle apparecchiature elettriche ed elettroniche utilizzate da persone giuridiche, pubbliche

[26] Tale aspetto potrebbe essere almeno parzialmente ovviato a fronte dell'emanazione del regolamento europeo sulla Privacy, attualmente in fase di approvazione.

amministrazioni, altri enti o persone fisiche nello svolgimento delle proprie attività e contenenti dati personali o sensibili.

- Tale provvedimento prevede l'adozione di misure tecniche preventive per la memorizzazione sicura dei dati, come ad esempio cifratura di singoli file o gruppi di file, e di misure specifiche per la cancellazione od oscuramento dei dati , come ad esempio l'utilizzo di appositi programmi informatici, la formattazione "a basso livello" delle apparecchiature o la demagnetizzazione dei dispositivi. Qualora non fosse garantita la non intelligibilità dei dati con le tecniche di cancellazione utilizzate, il dispositivo non può essere riassegnato e deve essere distrutto mediante procedure di punzonatura, deformazione meccanica, disintegrazione o demagnetizzazione ad alta intensità.
- L'introduzione dei dispositivi mobili, quali smartphone e tablet, utilizzati in modo sempre più diffuso, rende necessaria una particolare attenzione per le operazioni di riciclo e reimpiego dei dispositivi, che comportano un elevato livello di rischio di rinvenimento di dati personali e sensibili da parte di soggetti non incaricati del trattamento.
- Pertanto è fondamentale che siano scelte delle soluzioni di sicurezza e dei processi di gestione in grado di garantire la rimozione sicura dei dati presenti nei dispositivi dismessi / riassegnati e l'impossibilità di accedere agli stessi finché essi sono presenti sul dispositivo: per le misure in tal senso si vedano le successive misure idonee di sicurezza correlate all'adozione di misure crittografiche di protezione.

- Il Gruppo di Lavoro inoltre evidenza la criticità di rimuovere non solo i dati effettivamente presente sui dispositivi, ma anche tutti gli elementi correlati (link, cookies, client…) in grado di permettere il raggiungimento di informazioni presenti su servizi esterni (ad esempio di clouding).

Misure idonee di sicurezza

Come illustrato nei capitoli precedenti, la normativa attuale, pur non prevedendo specifiche misure di sicurezza applicabili all'ambito operativo dei dispositivi mobili evoluti, indica già alcuni elementi di protezione dei dati personali trattati di natura tecnologica, organizzativa e procedurale che compongono un layer minimo di requisiti mandatori a cui attenersi.
Ciononostante nella maggior parte dei casi, essendo di natura generale e minima, tali misure non sono sufficienti a proteggere opportunamente i dati trattati. Per questo motivo, la normativa stessa prevede che le società che trattano dati personali identifichino quelle che, a buon ragione, possono essere ritenute delle misure idonee. In particolare tale aspetto è introdotto dall'art.31 del Codice Privacy che riporta:

> *"Art. 31- I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".*

Ovviamente l'identificazione di tali misure deve scaturire da opportune iniziative di valutazione dello specifico contesto operativo dei trattamenti effettuati, promosse dal titolare e/o dai responsabili dei trattamenti. Tali valutazioni consistono sostanzialmente nell'attività periodica di analisi dei rischi, così come indicato all'art.34 del Codice Privacy, che, prendendo in considerazione le attività operative ed i rischi specifici correlati al contesto di utilizzo dei dispositivi mobili evoluti, permettono di determinare il livello di protezione dei dati trattati e le eventuali misure di sicurezza da adottare al fine di rafforzare tale aspetto. La suddetta analisi dei rischi era finora generalmente effettuata nel contesto di predisposizione del Documento Programmatico Sulla Sicurezza (DPS), documento attualmente oggetto di revisione normativa, sia a livello nazionale che di Comunità Europea, come evidenziato in precedenza. A fronte di tali modifiche normative, sarà necessario stabilire secondo quali modalità ed in quali contesti realizzare tale analisi. A prescindere comunque dalla sua formale collocazione, tale elemento risulta comunque fondamentale per ovviare anche ad aspetti rilevanti quali:

- la difficoltà intrinseca di valutazione del proprio portafoglio tecnologico, in considerazione della quantità e tipologia di dispositivi mobili che possono esistere nell'ambito aziendale, volendo considerare anche i sistemi di proprietà dei dipendenti/collaboratori ecc.;
- la carenza di linee guida consolidate sull'argomento: sebbene negli ultimi tempi si siano resi disponibili numerosi studi e valutazioni in merito alla sicurezza dei dispositivi mobili, sia da parte di enti autorevoli (ENISA, NIST, ISACA), che da parte di soggetti privati competenti sul tema, si tratta spesso di considerazioni valide ma troppo generiche o, viceversa troppo orientate a situazione specifiche.

Nonostante quanto evidenziato sopra, ovvero che le misure idonee siano correlate all'analisi dei rischi del contesto operativo, il Gruppo di Lavoro ha ritenuto che alcune misure possano essere comunque identificate quali particolarmente rilevanti (e quindi sostanzialmente necessarie), tenendo in considerazione che quasi tutti i contesti delle aziende presentano le seguenti caratteristiche:

- presenza nel perimetro aziendale di smartphone, sia aziendali che privati, con accesso ai sistemi ed ai servizi IT aziendali;
- trattamento di dati personali mediante tali dispositivi (ivi inclusa una possibile memorizzazione);
- possibilità che un incidente ai dati trattati mediante i dispositivi possa propagarsi ed interessare anche gli ulteriori ambiti tecnologici aziendali

Date tali caratteristiche comuni è quindi possibile ipotizzare che esistano delle misure idonee comuni ai diversi contesti operativi. Tali misure verranno descritte di seguito, evidenziandone la natura tecnologia, organizzativa o procedurale.

Misure di natura prevalentemente organizzativa e procedurale

Le misure di natura organizzativa e procedurale hanno l'obiettivo di gestire opportunamente i rischi correlati alla sicurezza dei dati e delle informazioni. Tra di esse il Gruppo di Lavoro evidenzia:

- le misure di formazione verso gli utilizzatori dei dispositivi mobili evoluti e di chi ne gestisce l'infrastruttura correlata;
- la definizione di opportuni modelli organizzativi preposti alla sicurezza dei dati e delle informazioni, con eventuali ruoli dedicati al governo dei dispositivi e/o delle infrastrutture centralizzate correlate;
- l'adozione di policy dedicate all'utilizzo dei dispositivi e/o alla loro gestione.

Tali misure sono di fatto valide per qualsiasi contesto tecnologico e la loro specifica applicazione all'ambito dei dispositivi mobili evoluti può essere attuata da parte delle società secondo approcci diversi, tenendo in considerazione la numerosità e la rilevanza di tali dispositivi nel contesto dei processi di business (diversa è la necessità di avere delle risorse dedicate responsabili della gestione del portafoglio mobile, ad esempio, per una società di agenti di commercio che quella relativa ad una società in ambito industriale…) e le ipotesi di *spending* e di investimenti fatte dalla società. Considerati gli aspetti di rilevanza e di peculiarità in ambito *mobile*, il Gruppo di Lavoro ha determinato di approfondire l'elemento relativo all'adozione di policy di sicurezza..

a. Information Security Policy Architecture (ISPA)

Uno degli elementi preponderanti per garantire una opportuna e strutturata *Governance* degli aspetti di sicurezza dei dati e delle informazioni è l'adozione di un'architettura di policy di sicurezza (o Information Security Policy Architecture ISPA). Tale architettura deve includere e indirizzare tutte le principali aree di protezione delle informazioni, le quali possono essere inquadrate secondo due direttrici:

- verticalmente, sulla base del livello di profondità e dettaglio delle tematiche trattate, prevedendo pertanto l'esistenza di policy di alto livello che definiscono i principi di sicurezza a cui attenersi, fino ad istruzioni o procedure operative, che indicano le specifiche modalità con cui realizzare le diverse attività;
- orizzontalmente, sulla base delle tematiche specifiche trattate (e.g. controllo accessi, gestione delle operation, …).

Nel contesto di tale sistema di policy il Gruppo di Lavoro ritiene che si debbano inserire anche opportune policy di diverso livello contenenti le regole correlate ai dispositivi mobili evoluti ed a tutti gli aspetti correlati (Apps installabili, modalità di connessione autorizzate, modalità di conservazione e trasferimento dei dati personali…).

Oltre a quanto già evidenziato in precedenza[27], tali policy dovrebbero tenere in considerazione aspetti concernenti sia gli utilizzatori sia i gestori dei dispositivi nonché di eventuali contesti tecnologici strettamente correlati (e.g. servizi di cloud computing), definendo:

- ruoli e responsabili dei diversi referenti che effettuano la gestione di tali dispositivi;
- modalità di attuazione dei diversi aspetti di gestione per lo specifico ambito mobile (e.g. gestione misure antimalware, gestione dei backup, gestione dei processi di assegnazione, modalità del controllo accessi…);
- responsabilità degli utenti nel corretto utilizzo di tali dispositivi (ivi inclusa la definizione di opportuni elementi sanzionatori)

Nel contesto di ciascuna policy, dovrebbero essere definiti chiari obiettivi, il campo e lo scopo di applicazione, il ciclo di vita e la gestione della policy stessa. Inoltre sarebbe opportuno valutare i rischi legati all'introduzione e gestione complessiva dei dispositivi mobili e le misure di sicurezza necessarie quali ad esempio:

- meccanismi di autenticazione per inibire l'uso di dispositivi persi o rubati;
- crittografia di file/cartelle per impedire la rilevazione non autorizzata di dati;

[27] Si veda il capitolo degli adempimenti formali in riferimento agli aspetti dell'informativa.

- backup e restore per proteggersi dalla perdita di dati personali;
- comunicazione sicura per arrestare l'intercettazione e l'accesso backdoor alla rete;
- firewall mobili per inibire gli attacchi wireless contro i dispositivi;
- antivirus mobile e ID per rilevare e impedire la compromissione del dispositivo;
- autorizzazione dell'interfaccia e delle applicazioni all'installazione di programmi di controllo, all'uso della rete, alla sincronizzazione e al data trasfer da e verso i dispositivi di storage rimovibili.

Le aziende dovrebbero considerare e formalizzare gli aspetti legati ai processi di censimento dei dispositivi mobili e dei software aziendali permessi, ai relativi processi di deployment, agli aspetti formativi relativi a gestoried utilizzatori e prevedere processi di auditing e monitoring.

La definizione di specifiche policy e procedure di sicurezza specifiche per l'ambito mobile deve essere in linea con i principi generali di sicurezza adottati dall'azienda per non introdurre elementi di discontinuità rispetto a questi e al livello compliance generale. In particolare si ritiene opportuno che gli aspetti peculiari dell'ambito mobile siano introdotti nella policy utenti e nelle policy di gestione che presentano degli elementi specifici per tali dispositivi (backup, antimalware…)

Misure di natura prevalentemente tecnologica

b. Remote wiping

Le preoccupanti statistiche relative alla perdita per smarrimento o furto dei dispositivi ed all'accesso non autorizzato a dati ed informazioni (in relazione anche ad attività di manutenzione, riassegnazione e smaltimento dei dispositivi) rendono particolarmente rilevante l'adozione in ambito aziendale di misure tecnologiche correlate[28]. Tra le misure di maggiore importanza ci sono quelle relazionate alle soluzioni di *wiping*.

A parte alcune differenze tipiche delle varie piattaforme presenti sul mercato, le misure di wiping consistono, in generale, in soluzioni tecnologiche di diversa complessità, che prevedono l'attuazione di comandi (da remoto o dirette sui dispositivi) per la cancellazione dei dati e delle informazioni (mail e suoi allegati, foto, contatti, sms, agenda, ecc...) presenti sul dispositivo.

Considerando il valore dei dati trattati e le statistiche sulla frequenza dei furti e degli smarrimenti dei dispositivi *mobile*, è facilmente comprensibile come l'attuazione di tali misure da remoto (in tal caso ci si riferisce a misure di *remote wiping*) sia particolarmente rilevante e, quindi, come tali misure siano da ritenere a tutti gli effetti misure non solo idonee, ma indispensabili. Tra le soluzioni di remote wiping è possibile identificare:

- soluzioni *built-in* ovvero soluzioni messe a disposizione nativamente nel dispositivo VS soluzioni applicative opportunamente installate sui dispositivi;
- soluzioni gestite internamente all'ambito aziendale ovvero soluzioni demandate in outsourcing ad opportuni soggetti tecnologici terzi…

Tale eterogeneità di soluzioni è illustrata, a titolo di esempio, per le principali piattaforme, nella tabella riportata sul sito del Gruppo di Lavoro[29], che tiene altresì in considerazione le soluzioni per i dispositivi ad uso privato e quelli ad uso aziendale.

Dalle soluzioni riportate nella suddetta tabella, appare evidente che, indipendentemente dalla piattaforma, le soluzioni tecnologiche a supporto della protezione dei dati presenti su dispositivi *mobile* funzionano tipicamente appoggiandosi ad un servizio web, su cui si crea

[28] È bene evidenziare inoltre che l'adozione di tali misure è, in alcuni ambiti operativi / per alcune attività, altresì mandatoria: si pensi ad esempio al suddetto Provvedimento del Garante del 13 ottobre del 2008 che rende obbligatoria (quindi non solo "Idonea") la rimozione dei dati presenti su dispositivo. Rimozione che in ambito mobile è da effettuare sia sulla memoria interna del dispositivo, che sui supporti esterni ed anche sulla SIM come visto in precedenza.

[29] http://privacycloudmobile.clusit.it/pages/Download.html

un account associato al dispositivo *mobile,* che dialoga con una componente client presente (di default o installata come App) sul dispositivo e che permette di eseguire le seguenti funzionalità:

- geolocalizzazione del dispositivo[30];
- eventuale backup dei dati presenti sul dispositivo su elementi centralizzati;
- eventuale comandi di *wiping* automatici del dispositivo in caso di tentativo di sostituzione SIM;
- comandi di *wiping* manuale dei dispositivi;
- *lock* del dispositivo;
- comparsa messaggi sullo schermo;
- *ring* del dispositivo.

Un'eventuale adozione di una policy di sicurezza aziendale, così come illustrata in precedenza, dovrebbe dunque anche prevedere la comunicazione relativa alle funzionalità offerte ai dispositivi *mobile* consegnati con le suddette funzionalità, affinché gli utenti ne siano consapevoli e le modalità per attivare tali funzionalità.

Allo stesso tempo eventuali policy di gestione dei dispositivi dovrebbero prevedere:
- l'eventuale creazione degli account in caso di servizio web (alla consegna del dispositivo);
- il backup periodico da remoto dei dati personali e/o sensibili;
- la predisposizione dell' accesso al servizio web per attivazione wiping automatico in caso di sostituzione SIM;
- l'immediato accesso al servizio web per attivazione wiping manuale in caso di smarrimento o furto del dispositivo.

In particolare si reputa che l'ultimo elemento meriti una particolare attenzione: l'accesso immediato per l'attivazione del *wiping* manuale è infatti fondamentale per garantire la corretta riduzione del rischio legato alla disponibilità dei dati sul dispositivo e quindi al loro accesso non autorizzato, tenendo conto che nella maggior parte delle soluzioni, è richiesto che per attuare, il dispositivo stesso debba essere acceso e connesso ad una rete. Appare ovvio infatti che più tempo passa e maggiori sono le possibilità (soprattutto in caso di smarrimento) che il dispositivo venga spento e, soprattutto, non più acceso. In tal senso è quindi fondamentale che l'adozione di tali misure sia fortemente integrata con i processi di incident management adottati in ambito aziendale.

Infine, si ritiene che l'attuazione delle suddette misure non possa prescindere da un corretta serie di istruzioni verso gli utenti dei dispositivi (policy utenti) a cui attenersi per proteggere opportunamente i dati presenti nel dispositivo e non solo nel caso di perdita o smarrimento, ma più in generale in caso di necessità di rimuovere i dati sul dispositivo (si pensi ad esempio ai dispositivi utilizzati in ambiti operativi che prevedono turni, condivisi da più utenti…).

L'adozione pertanto di soluzioni di wiping ed in particolare di remote wiping possono essere ritenute critiche ai fini di proteggere opportunamente i dati personali trattati mediante i dispositivi mobili, soprattutto relativamente ai casi di smarrimento / furto dei dispositivi.

Affinché tali soluzioni siano attuate in maniera efficace, è altresì fondamentale che esse siano strettamente correlate ai processi di incident management aziendali adottati in azienda, affinché siano prontamente attivate in caso di smarrimento/ furto del dispositivo.

[30] Anche per tale motivo l'opportuna gestione dei dati di geolocalizzazione dei dispositivi assegnati ai dipendenti deve essere effettuata nel rispetto degli adempimenti formali visti nei capitoli precedenti.

c. Encryption

In caso di smarrimento o furto del dispositivo *mobile*, le soluzioni di wiping descritte in precedenza hanno tutte una limitazione in comune: per funzionare richiedono il raggiungimento da remoto del dispositivo, tramite reti pubbliche. In caso di furto, è possibile (e si ritiene molto probabile) che tale limitazione sia ben nota all'individuo che ha sottratto il dispositivo e pertanto ha senso ipotizzare che se l'attivazione di tali soluzioni non avviene prontamente, l'efficacia delle stesse possa rapidamente decrescere. Il malintenzionato potrebbe, infatti, disconnettere il dispositivo dalla rete e/o rimuovere le eventuali memorie di massa rimovibile (SD, MMC, ecc..), per inserirle in un nuovo dispositivo compatibile o in un lettore e, mediante opportuni tools, disporre delle informazioni in esso contenute.

Le specifiche prescrizioni per questi ambiti particolari e, soprattutto, le considerazioni di rischio indicate in precedenza determinano come l'adozione delle misure di protezione crittografica dei dati presenti sui dispositivi, possa di fatto essere ritenuta fondamentale non solo laddove sussista il suo carattere obbligatorio (ad esempio in relazione ai trattamenti di dati genetici e/o di dati sanitari per il fascicolo elettronico sanitario), ma anche ai fini di un'opportuna protezione dei dati personali contenuti e trattati.

Determinata quindi l'importanza, si tratta di capire come governarne l'adozione. Dati, infatti, i trend evidenziati nei capitolo iniziali, quali la possibilità che esistano dei portafogli estesi di dispositivi da gestire in ambito aziendale o l'attuazione degli approcci BYOD, la scelta delle soluzioni più adeguate può non essere semplice, né tanto meno i successivi aspetti di gestione (che comportano, ad esempio, la gestione delle chiavi crittografiche).

Se infatti molte piattaforme tecnologiche hanno già nativamente la possibilità di attivare tali soluzioni (soluzioni *built-in*), è altresì vero che tale indicazione non è sempre vera. In questi casi può sopperire l'adozione di specifiche Apps che consentono di attivare questa funzionalità con un elevato livello di sicurezza.

Pertanto la corretta adozione di tali soluzioni, dovrebbe essere correlata ad un processo strutturato di valutazione dei rischi e delle diverse alternative, che tenga conto almeno seguenti elementi:

- identificazione di soluzioni, qualora non built-in, compatibili con il portafoglio dispositivi adottato a livello aziendale;
- modalità di installazione delle soluzioni, tenendo in considerazione l'esistenza di eventuali situazioni di uso misto, di strategie BYOD per i dispositivi mobile consegnati ai dipendenti;
- definizione delle basi di dati (mail, rubrica, password, cartelle, ecc..) e/o degli elementi tecnologici (SIM, memoria del dispositivo, SD/MMC, ecc) su cui applicare le misure di cifratura, valutando pienamente ed attentamente il compromesso con le performance del dispositivo (se si decide di cifrare tutto, alcune operazioni potrebbero essere rallentate) e l'operatività in generale. Ad esempio, se di decide di cifrare la rubrica, in alcuni casi potrebbe non funzionare il riconoscimento del Caller;
- configurazione delle soluzioni secondo criteri di cifratura definiti;
- successiva gestione delle chiavi crittografiche così generate (conservazione, utilizzo delle stesse in caso di incidenti sui dispositivi…);
- consegna ai dipendenti di chiare istruzioni operative per non disabilitare inavvertitamente le funzionalità di cifratura (non potendo spesso inibire privilegi amministrativi sul dispositivo).

Relativamente alle principali soluzioni esistenti per le diverse piattaforme tecnologiche, si rimanda alla tabella riportata alla pagina web già citata in precedenza[31].

[31] http://privacycloudmobile.clusit.it/pages/Download.html

Affinché i dati personali presenti su dispositivo siano pienamente protetti da accessi non autorizzati in relazione ad eventi di smarrimento / furto si ritiene fondamentale l'adozione di misure di cifratura degli stessi. L'adozione di tali misure determina la necessità di indirizzare una serie di aspetti correlati, con particolare attenzione alla selezione delle soluzioni coerenti con l'ambito tecnologico e la definizione delle chiavi crittografiche.

d. I sistemi MDM/MDA

La gestione del portafoglio dei dispositivi mobili in ambito aziendale può risultare particolarmente difficoltosa, sia per la natura stessa dei dispositivi, sia per l'eterogeneità del portafoglio degli stessi, che può rendere problematica l'implementazione di un opportuno ed uniforme livello di protezione dei dati trattati.

Al fine di garantire tale livello di sicurezza è quindi essenziale l'adozione di una strategia di gestione strutturata e complessa, composta da procedure, processi e tecnologie, in grado di far governare in maniera accentrata i vari aspetti di sicurezza e di limitarne i costi.
Per venire incontro a queste esigenze sono nati i sistemi di *Mobile Device Management* (MDM) talvolta accompagnati o integrati con sistemi di *Mobile Application Management* (MAM). Queste soluzioni consentono di centralizzare la gestione dei dispositivi (anche funzionanti con sistemi operativi differenti) fornendo al reparto IT gli strumenti necessari ad una gestione uniforme di diverse procedure legate alla sicurezza del dispositivo e del dato in esso contenuto.

I sistemi di MDM consentono di agire anche *on-the-air*, senza che il dispositivo debba essere collegato ad una postazione del gestore IT. Alcuni di questi sistemi necessitano di una componente *client* installata sul dispositivo, mentre altri utilizzano funzionalità standard messe a disposizione dal sistema operativo presente sul *device* stesso.

Le principali caratteristiche funzionali di un sistema MDM sono riepilogate nel seguente elenco, evidenziando in parentesi, laddove applicabili, anche i punti di riferimento del Disciplinare Tecnico (All.B):

- gestione delle credenziali e delle password - reset, verifica…(punti dell'All.B correlabili 5., 7., 8., 10.) ;
- verifica della configurazione del dispositivo (e.g. versione OS installato) e aggiornamenti remoti (pto.17)
- individuazione dispositivi con installati sistemi operativi non standard (es. iOS jailbreak);.
- disabilitazione servizi di condivisione dati;
- gestione backup dati, restore e degli aspetti di sicurezza correlati - crypting dei backup… (pto.18)
- limitazione delle attività / dei servizi DLP, quali, ad esempio possibilità di impedire backup di App aziendali e dei loro dati, limitazione connessioni, limitazione su navigazione internet, installazione App di soggetti terzi…pto.18)
- gestione delle schede rimovibili (crittografia, disabilitazione scrittura…);
- gestione delle installazioni remote di Apps aziendali;
- remote wiping / rimozione dei dati (pto.22);
- locking remoto del device (pti.7 e 8);
- integrazione con i sistemi aziendali di Identity Management;
- logging;
- GPS Tracking.

È comunque importante sottolineare che le funzionalità riportate non sono sempre disponibili per tutte le piattaforme. Sul mercato si trovano soluzioni che gestiscono specifici sistemi operativi oppure pacchetti che consentono la gestione di sistemi operativi eterogenei[32].

[32] L'Open Mobile Alliance (OMA) [http://www.openmobilealliance.org/Technical/DM.aspx] ha tra i propri obiettivi la definizione di un protocollo di gestione dei dispositivi che sia indipendente dalla piattaforma e che agevoli la realizzazione di strumenti trasversali.

Esistono principalmente tre modalità di implementazione e fruizione di un sistema MDM: gestione In-House, servizio Cloud/SaaS e servizio Outsourcing. In funzione delle esigenze e delle caratteristiche dell'azienda che intende adottare il sistema, la scelta può ricadere su una di queste modalità.

- Adottando una soluzione In-House l'infrastruttura hardware e lo strato software sono installati presso i locali dell'azienda stessa, che dovrà quindi occuparsi della manutenzione e della gestione dell'hardware e del software applicativo. Una soluzione di questo tipo ha il vantaggio di fornire il pieno controllo di tutto il sistema e della sua sicurezza, ma di contro comporta costi aggiuntivi in termini di acquisizione delle conoscenze inerenti la specifica piattaforma adottata, nonché dei costi relativi alle risorse umane da allocare per la gestione del nuovo sistema in ambiti evolutivi (si pensi ad esempio all'introduzione di nuove tipologie di device mobile) e di manutenzione, come ad esempio l'aderenza dell'infrastruttura a nuove normative in ambito sicurezza.
- Un approccio differente avviene con le soluzioni fornite come servizio Cloud/SaaS. In questo contesto l'azienda non ha più in carico la gestione dell'infrastruttura e della sua sicurezza, ma demanda tali attività al fornitore, mantenendo però il controllo applicativo (remoto) sul sistema MDM e sulla gestione dei device. Una soluzione di tipo Cloud vede quindi un coinvolgimento minore delle risorse dell'azienda a scapito di un minor controllo diretto del sistema.
- La terza soluzione prevede la gestione dell'intero sistema MDM in Outsourcing, demandando all'esterno dell'azienda non solo la gestione dell'infrastruttura e della sua sicurezza, ma anche le attività di controllo e gestione del prodotto MDM e dei dispositivi aziendali da esso gestiti. Questa soluzione consente all'azienda di usufruire dei benefici del sistema MDM senza la necessità di allocare ulteriori risorse nella gestione dello stesso. Rispetto alle soluzioni precedentemente descritte, l'Outsourcing diminuisce ulteriormente il controllo diretto del sistema.

Per quanto concerne le problematiche di Privacy del dato, è necessario introdurre un'ulteriore distinzione tra servizi Cloud/Saas e servizi in Outsourcing. Nel primo caso la definizione stessa di Cloud prevede che il fornitore possa elaborare i dati in località non definite a priori; e nel luogo di elaborazione potrebbe non essere garantita la medesima copertura normativa. In caso di Outsourcing, a meno che il fornitore stesso non si avvalga di servizi Cloud, il rapporto è più diretto e l'azienda cliente può avere un maggiore controllo sulla modalità di gestione dei propri dati.

In conclusione, un'azienda che decide di adottare un sistema MDM, oltre a verificare la copertura di differenti tipologie di device (iOS, Android, BlackBerry, ecc.) e le singole funzionalità che i fornitori implementano nei propri sistemi, deve prendere in considerazione anche diversi fattori della realtà aziendale (dimensione attuale, dimensione futura, livello di competenza del reparto IT, budget, ecc). Tutte le considerazioni devono poi essere rapportate e soppesate in funzione del livello di controllo che l'azienda vuole ed è in grado di avere sul sistema.

Si evidenzia infine che l'utilizzo di un sistema di *Mobile Device Management* ha un diretto impiego per quanto richiesto specificatamente dai provvedimenti relativi agli Amministratori di Sistema e alle Linee Guida per l'utilizzo di Internet.

Affinché vi sia una corretta e robusta gestione dei dispositivi mobili che garantisca un opportuno livello di sicurezza per i dati trattati, si ritiene opportuno che il portafoglio dispositivi sia gestito mediante soluzioni tecnologiche strutturate.

e. Sandbox/Hardening dei dispositivi

Fra le soluzioni di sicurezza che possono essere considerate per la protezione dei dati e delle informazioni trattati in ambito aziendale, è necessario prendere in considerazione anche quelle correlate a garantire la "qualità" del software utilizzato. Con questa espressione si fa riferimento al complesso di misure, approcci metodologici, procedure e strumenti concepiti per contrastare le vulnerabilità insite nel codice sorgente delle applicazioni adottate in ambito aziendale e generalmente già presenti nelle *best practice* e negli standard di sicurezza

relativi ai sistemi informativi aziendali (e.g. nello standard generale ISO/IEC 27001, o nello standard di settore PCI-DSS ad esempio).

Il Gruppo di Lavoro ritiene che tale insieme di misure siano particolarmente critiche per il contesto di trattamento di dati personali attraverso i dispositivi mobili evoluti, per i seguenti motivi:

- la quantità delle applicazioni potenzialmente fruibili dai sistemi *mobile* è ormai elevatissima e in fase di crescita continua;
- le modalità di reperimento delle Apps ne consentono l'installazione, in condizioni standard, con tempistiche minime;
- i sistemi di screening anti-malware messi in campo dai distributori delle apps non possono né potranno mai garantire da soli un livello di sicurezza sufficiente;
- i sistemi operativi dei sistemi mobili sono anch'essi in rapida evoluzione e con caratteristiche di sicurezza non sempre adeguate.

La conseguenza dei punti precedenti è che l'esposizione dei dispositivi mobili evoluti verso minacce correlate ad utilizzo di software infetto, vulnerabile ad attacchi o semplicemente malfunzionante è molto elevata e decisamente maggiore rispetto a quella riscontrabile nei parchi macchine dei sistemi informativi aziendali "convenzionali". Le soluzioni che indirizzano opportunamente i punti precedenti possono essere ricondotte a due categorie principali:

- soluzioni **preventive**, che hanno l'obiettivo di evitare o limitare l'adozione di Apps vulnerabili o infette (interventi sul ciclo di sviluppo del software applicativo) e/o di avvalersi di meccanismi di "reputation" e di trust nei confronti di sviluppatori e distributori;
- soluzioni **reattive**, ovvero di predisposizione di sistemi specifici per il rafforzamento dei sistemi operativi dei dispositivi.

Le contromisure **preventive** includono *best practice* già adottate per altri ambienti (per es. OWASP) e prevedono una serie di requisiti, quali, ad esempio, il controllo dei dati in input, l'utilizzo del principio di minimo privilegio, l'encryption dei dati trasmessi e memorizzati, la firma digitale dei binari ecc. A queste attività si devono affiancare l'*enforcement* dei test di sicurezza, l'utilizzo di sistemi di validazione a codice aperto e chiuso ed infine gli *application pen test*.
Complementare allo sviluppo sicuro delle Apps è il concetto di qualificazione degli sviluppatori e dei distributori di apps, attraverso un processo di peer review, in modo da favorire la reputazione di chi produce e veicola software con elevati standard di qualità e sicurezza.

Un metodo più radicale consiste nella limitazione forzata dell'utilizzo di software solo di specifici vendor (**walled gardens**).
Questo modello di prevenzione delle minacce si basa sul concetto di limitazione, a livello di distribuzione, delle applicazioni che possono girare sul dispositivo *mobile*. Questo viene effettuato attraverso un meccanismo di *enforcement* preventivo, basato ad esempio sulla combinazione di agenti software/applicazioni (o meglio su specifiche feature del sistema operativo) e di punti di distribuzione controllati per le applicazioni.

Il modello ideale è inoltre quello in cui prima della messa a disposizione delle applicazioni, il codice viene sottoposto a review attraverso meccanismi di analisi statica o dinamica. Una volta analizzato, lo stesso è quindi firmato digitalmente e infine messo a disposizione dell'utente secondo specifiche modalità guidate.
Il modello dei Walled Garden garantisce in teoria una *assurance* di sicurezza assai elevata, perché si pone l'obiettivo di garantire a priori un ecosistema di applicazioni esenti da minacce. D'altra parte tale modello ha dimostrato alcune debolezze, tra le quali si evidenziano:

- la possibilità di eludere i meccanismi di enforcement del sistema operativo (*jailbreaking* dei dispositivi);
- l'impraticabilità di effettuare un check di sicurezza sul codice esaustivo, per evidenti motivi di tempo e risorse necessarie;
- la rigidità del modello, che può indurre l'utente stesso a cercare di spezzare i sistemi di enforcement.

Per questi motivi le aziende stanno prendendo in considerazione modelli di protezione alternativi, quali i già citati MDA e/o MDM.

Le contromisure **reattive** sono quelle che contrastano le attività offensive del malware, principalmente attraverso la corazzatura dei sistemi operativi e l'adozione di sistemi di esecuzione controllata delle Apps (**sandboxing**).

Questi concetti derivano dall'esperienza pregressa derivante ad esempio dal mondo dei desktop, dove sono apparsi subito evidenti i gravi problemi di sicurezza a cui poteva essere esposto un sistema informativo i cui client non erano in grado di esercitare uno stretto controllo sulle applicazioni eseguite. L'evoluzione dei sistemi operativi lato client ha solo parzialmente limitato il pericolo, in quanto le minacce si sono spostate nella ricerca di vulnerabilità del sistema operativo, nell'infiltrazione mediante tecniche di social engineering o nell'uso di sistemi di rootkit. Tutte queste tecniche sono volte a sovvertire le barriere imposte dai sistemi operativi alle applicazioni.

Le tecnologie di sandbox possono essere considerate come un ulteriore livello di protezione dei sistemi, in un'ottica di difesa in profondità. Il concetto cardine dei sandbox è la limitazione del *workspace* delle applicazioni, impedendo che possa violare o danneggiare le risorse o i dati delle altre applicazioni.
Nell'ambito dei sistemi *mobile* l'utilizzo delle tecnologie di sandbox è quindi particolarmente attraente, in considerazione delle specificità, descritte in precedenza, di questi scenari. Tuttavia il paradigma dell'isolamento applicativo è stato interpretato in modo differente dai fornitori di sistemi operativi. Il modello classico di sandbox è quello dove esistono due modi d'uso specifici (base e privilegiato) dove le applicazioni in modalità normale non possono accedere agli oggetti riservati alle applicazioni in modalità privilegiata. Tuttavia le applicazioni che "girano" in modalità base condividono fra di loro l'accesso agli stessi oggetti (ad esempio file). Nei modelli più avanzati di sandbox ogni applicazione è segregata in modo da poter accedere ad un set esclusivo di oggetti, con funzionalità comuni ridotte al minimo. Questo modello di isolamento applicativo è adottato ad esempio da iPhone ed Android. Questi OS "etichettano" ogni applicazione con uno specifico ID e ne assicurano l'isolamento di dati e processi dalle azioni delle altre apps.
Viceversa altri sistemi si affidano su un modello più tradizionale dell'isolamento applicativo, di solito accoppiato con sistemi di "firma" delle applicazioni. Questo significa che a determinate applicazioni il sistema operativo concede l'esecuzione in modalità privilegiata, previa verifica della sua integrità e autenticità mediante la verifica della firma digitale. L'applicazione deve quindi essere firmata digitalmente e l'autenticità della firma assicurata mediante certificati digitali. Il sistema operativo deve ovviamente essere dotato (in modo nativo o mediante specifiche applicazioni) della capacità di verificare i certificati.

Conclusioni

Il presente documento ha cercato di analizzare uno specifico ambito dei possibili trattamenti di dati personali effettuati tramite dispositivi mobili evoluti (smartphone e tablet), ovvero quelli realizzati in ambito aziendale, da parte di personale incaricato.
Le osservazioni articolate hanno evidenziato che affinché siano garantiti tanto il raggiungimento dei benefici attesi, quanto un opportuno livello di protezione dei dati trattati, è quanto meno necessario che siano considerati tutti i requisiti esplicitamente presenti nell'attuale normativa Privacy italiana. Le misure minime di sicurezza (controllo degli accessi, salvataggio dei dati trattati…) e gli adempimenti formali (informative, notificazioni…) per cui è richiesta esplicita conformità devono però essere presi in considerazione, cercando di individuarne gli aspetti peculiari dell'ambito *mobile*. Le normative attuali sono infatti maggiormente focalizzate su contesti tecnologici solo parzialmente adatti alle specificità introdotte dai dispositivi mobili evoluti.

Le evoluzioni normative in atto, tanto a livello italiano, quanto a livello comunitario, rappresentano un'opportunità affinché siano opportunamente recepiti ed indirizzati dalle norme gli aspetti innovativi del nuovo trend tecnologico.
Allo stesso tempo però, per quanto il contesto regolatorio non sia pienamente allineato a quello tecnologico, è stato evidenziato che la corretta realizzazione dei suddetti trattamenti, non può limitarsi a considerare i soli aspetti normativi esplicitati, ma come sia necessario che siano altresì adottate quelle misure indicate quali idonee, ovvero quelle misure che, pur non essendo richieste puntualmente, sono le sole a garantire un adeguato livello di protezione dei dati. L'identificazione di tali misure è subordinata alla definizione ed alla periodica realizzazione di un attività di analisi dei rischi che, considerando lo specifico contesto operativo e le minacce ad esso correlato, permetta di identificare le aree maggiormente critiche e di conseguenza le opportune soluzioni per gestirle. L'importanza di tale analisi dei rischi e della scelta delle opportune misure idonee risulta ancor più rilevante ed evidente, considerando diversi elementi caratterizzanti l'adozione di tali dispositivi, quali, ad esempio:

- l'eterogeneità del panorama dei dispositivi, caratterizzati da elementi tecnologici anche molto diversi;
- la complessità delle soluzioni e dei trend in atto, che comprendono sia l'affermazione di soluzioni più strutturate e omogenee sia approcci che prevedono esplicitamente la perdita di governo di alcuni aspetti (e.g. BYOD), a favore del rafforzamento di altri aspetti di sicurezza;
- l'estrema rapidità con cui sta evolvendo il settore, in cui features e servizi realizzabili con i dispositivi stanno crescendo esponenzialmente, rendendo di fatto i trattamenti effettuati con tali dispositivi sempre più appetibili ai fini di business;
- l'affermazione di ulteriori elementi facilitatori, quali il rafforzamento delle infrastrutture di connettività mobile, attraverso l'introduzione del nuovo standard LTE e la delocalizzazione dei dati con le soluzioni di cloud computing.

Allo stesso tempo il Gruppo di Lavoro è conscio che le tematiche trattate sono solo una parte di tutti gli aspetti che correlano dati personali, Privacy e *mobile* e si augura quindi che anche gli ulteriori ambiti possano essere oggetto di successivi approfondimenti. Tematiche, infatti quali il trattamento dei dati personali ricevuti dai dispositivi mobili evoluti dei clienti, la gestione e la realizzazione di attività promozionali su tali dispositivi o il trattamento di tutti i dati originati da tali dispositivi da parte degli operatori del settore delle telecomunicazioni o di quei soggetti che offrono i servizi VAS (Value Added Services) saranno infatti ambiti di assoluta importanza nel breve periodo e pertanto degni di opportune analisi ed esplorazioni.

Autori e contributori

Questo lavoro è frutto della collaborazione delle seguenti aziende, studi legali e associazioni

Team Leader ed editor

Brera Jonathan, KPMG – Manager Information Risk management. CISA, CISM, CRISC, L.A.ISO27001, L.A. BS25999, Prince2 Foundation, socio ISACA e AIEA

Vallega Alessandro, Oracle – Security Business Development, Coordinatore di Oracle Community for Security, Consiglio Direttivo Clusit, membro AIEA

Autori e contributori

Abeti Riccardo, Studio Abeti – Presidente della Commissione "New Technology, Personal Data and Communication Law" e membro del Comitato esecutivo dell'Unione Avvocati Europei

Borgonovo Alberto, KPMG – Manager Information Risk management. CISA, CRISC, L.A.ISO27001, ITILv3, Prince2, OPST, socio ISACA e AIEA

Ciabattini Enrico, Ernst & Young – Senior IT Risk & Assurance Services

Fragnito Angelo, Business-e – Senior Security consultant, L.A.ISO27001, ITIL v3

Fumagalli Sergio, Zeropiù – VicePresident, responsabile relazioni esterne e partnership, coautore di "Privacy guida agli adempimenti", pubblicato da Ipsoa

Indovina Barbara, Array – Avvocato, professore a contratto c/o Univ.Commerciale L.Bocconi "Informatica per Giurisprudenza"

Leone Roberto, Spike Reply – Senior Security Consultant; progetti di sicurezza in ambito tecnologico e GRC. Responsabile linea di offerta sulla security dei digital process

Librera Paolo, Zeropiù – Technical account manager – Responsabile progetti di sicurezza in ambito IAM e *mobile*

Mariotti Andrea, Ernst & Young – Senior Manager IT Risk & Assurance Services. CISA, CISM, CRISC, L.A.ISO27001, L.A.ISO20000, socio AIEA e AIPSA

Pisacane Francesco, KPMG – Project Leader, Information Risk Management. CRISC, L.A. ISO 27001, L.A.BS25999 ITIL V.3, Silver member ISACA e socio AIEA

Prampolini Natale, **AIEA** – Senior Consultant, Socio e Proboviro AIEA, CISA, CISM, L.A. ISO27001, L.A. ISO20000, ITILv3, COBIT 4.1, CMMI 1.2 DEV

Squilloni Valentino, Spike Reply – Business Development Manager Large Account; gestione vendor/partner tecnologici di riferimento per la Security

https://privacycloudmobile.clusit.it/