COMMISSIONE IX
TRASPORTI, POSTE E TELECOMUNICAZIONI

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

2.

SEDUTA DI MARTEDÌ 15 MAGGIO 2012

PRESIDENZA DEL PRESIDENTE **MARIO VALDUCCI**

INDICE

N. B. Sigle dei gruppi parlamentari: Popolo della Libertà: PdL; Partito Democratico: PD; Lega Nord Padania: LNP; Unione di Centro per il Terzo Polo: UdCpTP; Futuro e Libertà per il Terzo Polo: FLpTP; Popolo e Territorio (Noi Sud-Libertà ed Autonomia, Popolari d'Italia Domani-PID, Movimento di Responsabilità Nazionale-MRN, Azione Popolare, Alleanza di Centro-AdC, La Discussione): PT; Italia dei Valori: IdV; Misto: Misto; Misto-Alleanza per l'Italia: Misto-ApI; Misto-Movimento per le Autonomie-Alleati per il Sud: Misto-MpA-Sud; Misto-Liberal Democratici-MAIE: Misto-LD-MAIE; Misto-Minoranze linguistiche: Misto-Min.ling.; Misto-Repubblicani-Azionisti: Misto-R-A; Misto-Noi per il Partito del Sud Lega Sud Ausonia: Misto-NPSud; Misto-Fareitalia per la Costituente Popolare: Misto-FCP; Misto-Liberali per l'Italia-PLI: Misto-LI-PLI; Misto-Grande Sud-PPA: Misto-G.Sud-PPA.

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE MARIO VALDUCCI

La seduta comincia alle 10,30.

(La Commissione approva il processo verbale della seduta precedente).

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso l'attivazione di impianti audiovisivi a circuito chiuso, la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-tv* della Camera dei deputati.

Audizione dell'amministratore delegato di Poste Italiane Spa, Massimo Sarmi.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza informatica delle reti, l'audizione dell'amministratore delegato di Poste Italiane Spa, Massimo Sarmi.

Do la parola all'ingegner Sarmi per lo svolgimento della relazione.

MASSIMO SARMI, *Amministratore delegato di Poste Italiane Spa*. Ringrazio per l'invito, perché Poste italiane si interessa di questi temi. Come ho avuto modo di accennare prima, non possiamo che partire dalla nostra storia.

È gradita l'occasione per ricordare che Poste italiane ha compiuto recentemente centocinquant'anni. È stata costituita, infatti, nel 1862 e, come capita in queste circostanze, andando a rivedere la storia, ci si ritrova nelle proprie origini e la missione attuale si confronta con la storia del passato.

Ricordiamo che nel 1862 si riuniscono le poste degli Stati precedentemente esistenti, se ne razionalizza la rete e gli uffici postali passano dagli allora 2.000 circa ai 14.000 circa di oggi.

Non sto a rappresentare fatti di natura logistica, ma l'impegno nei servizi logistico-postali viene affiancato a quello dei servizi finanziari. Già nel 1875, col Governo di Quintino Sella, nasce il libretto di risparmio postale.

Arriviamo al 1917, durante la Grande Guerra, quando si introducono il conto corrente postale e successivamente i prodotti del risparmio postale, ragion per cui le Casse di risparmio postale, che nascono nella seconda metà dell'Ottocento, si alimentano di nuovi prodotti. Da sempre la missione di Poste è quella di essere sul territorio e di offrire servizi essenziali.

Andiamo a vedere nello specifico il tema della comunicazione. La nostra missione sembra, per i suoi aspetti, un po' diversa da quella che ho descritto inizialmente, ma in realtà si intuisce come l'integrazione delle reti, fisiche, informatiche e logistiche, attribuisca un valore in più all'infrastruttura di Poste italiane nell'erogazione dei servizi. Il perno del funzionamento, l'abilitatore del funzionamento, è l'infrastruttura di *information and communication technology*.

Vediamo in sintesi le caratteristiche dell'infrastruttura, con i relativi numeri, sotto un profilo sia di fisicità, sia di caratteristiche di telecomunicazioni e informatica. Questa infrastruttura si prefigge lo scopo, oltre che di assicurare il funzionamento dei servizi e delle piattaforme di servizio, anche di permettere –

ed è una caratteristica di Poste italiane – di accedere ai servizi con le modalità che il cliente stesso può scegliere.

In altre parole, uno stesso servizio – uno dei più semplici è tipicamente il servizio di pagamento – può essere effettuato in fisicità, con un rapporto di uno a uno all'ufficio postale, via *web*, con il telefonino, che è un altro modo di rientrare nel mondo del *web*, al telefono, o ancora, e lo stiamo sperimentando, sul digitale terrestre. In generale, nel mondo televisivo, ciò è possibile abilitando gli schermi delle televisioni cosiddette *smart* per le funzionalità di servizio.

La novità è che la rete dei portalettere è anch'essa abilitata – in quanto dotata di strumenti collegati alle infrastrutture di rete – a portare i servizi a casa delle persone o negli uffici. È una novità in termini assoluti, che permette di declinare anche in maniera nuova ed aggiuntiva le modalità del servizio tradizionale. Il portalettere porta i servizi dell'ufficio postale a casa, ma è anche uno strumento disponibile per soggetti terzi ai fini dell'erogazione dei propri servizi, che possono essere servizi di utilità sociale, come la consegna dei farmaci a casa, o legati alle attività delle aziende. Si tratta di un'infrastruttura nuova, abilitata nel mondo delle telecomunicazioni mobili e collegata al resto dei sistemi.

Osservate la rappresentazione a nuvole, che non nasceva per questo scopo, bensì per una descrizione di sintesi delle infrastrutture, ma che rievoca sicuramente il concetto di *cloud computing*. Esso oggi rappresenta, a mio avviso, una realtà, oltre che una prospettiva, che può permettere l'evoluzione dei servizi soprattutto per il nostro tessuto industriale di aziende prevalentemente di medie e di piccole dimensioni, proprio per offrire in logica *cloud* infrastrutture di servizi in modalità sicura e naturalmente utili per lo svolgimento delle attività tipicamente logistico-amministrative delle aziende.

Sappiamo che oggi il cuore di un'infrastruttura di questo tipo sta nei cosiddetti *data center*. Dobbiamo ancora, ahinoi, superare il tema dell'interconnessione ad alta velocità, ma già si pone un tema di grande attualità, a mio avviso: la ricchezza nuova che viene espressa in termini di *information and communication technology* dalla rete e dalla caratteristica dei *data center*.

I data center, nel concetto cosiddetto di *open data*, che so essere oggetto di studio e di approfondimento anche a livello di Governo, sono quelli che permettono, con le dovute riservatezze, di utilizzare i dati, di integrarli e di incrociarli per offrire possibilità di servizio che altrimenti non sarebbero accessibili a piccole e medie organizzazioni. In altre parole, i dati costituiscono il vero patrimonio, il vero valore di un Paese moderno e possono essere combinati, declinati e integrati sotto un profilo di regole e di utilità.

In questo senso Poste italiane è all'avanguardia. Possiamo contare su cinque *data center* e nella prossima estate andremo a inaugurarne uno a Torino, che si correla e si coniuga con il concetto di *smart city*, in quanto da questo *data center* verranno offerti servizi in logica *cloud computing* nella modalità più evoluta.

Inoltre, abbiamo costituito i presupposti, con l'acquisizione del terreno e la progettazione, per un *data center* a Benevento, che viene a rispondere all'ampliata presenza geografica di Poste italiane. Vedete rappresentate nelle *slide* alcune caratteristiche di sintesi di questa importantissima infrastruttura.

Tutto ciò ci permette di seguire il flusso dello svolgimento dei servizi sia in logica tecnica, sia proprio in vista di come i servizi vengono percepiti dal cliente in tempo reale. I luoghi fisici che vengono rappresentati sono proprio gli ambiti in cui ogni giorno, ventiquattro ore su ventiquattro, viene seguito e gestito il flusso dei servizi, intervenendo in tempo reale laddove ci sono variabili, per esempio nella rete logistica, che suggeriscono il cambiamento.

Un aeromobile può non partire magari a causa del tempo. In tal caso si riprogramma in tempo reale un trasporto su gomma, in modo da far sì che la confluenza finale nella rete logistica avvenga.

Si esplora – a mano a mano arriviamo all'oggetto specifico dell'audizione in termini di sicurezza di funzionamento delle reti – tutto il mondo delle transazioni e delle operazioni che vengono effettuate sia nelle infrastrutture di Poste italiane, sia nel mondo più ampio e globale del *web*.

Entriamo ora nella rappresentazione di sintesi. A mio avviso, il concetto di un'infrastruttura di servizio deve potersi sviluppare secondo il seguente schema: innanzitutto si deve poter contare su un'infrastruttura di telecomunicazioni di base, alla quale è immediatamente annesso il concetto di disponibilità di banda di trasmissione in funzione della natura e della quantità dei dati che debbono essere rappresentati, ma subito sopra di esso dobbiamo immaginare uno strato di piattaforme di servizio.

Noi sappiamo che l'infrastruttura di per sé è condizione necessaria, ma non sufficiente per l'utilità verso i destinatari finali, siano essi persone, amministrazioni o aziende, e che tutto ciò avviene per il tramite di piattaforme di servizio che poi esamineremo. Basti immaginare la piattaforma di comunicazione elettronica, che può avere nella sua integrazione un riferimento con la corrispondenza tradizionale, in quanto da flussi elettronici si origina oggi la maggior parte della corrispondenza fisica.

Tutte le comunicazioni di natura commerciale che riceviamo nascono in genere da flussi elettronici che poi diventano corrispondenza fisica, oppure, al contrario, e ciò avviene sempre di più nell'ambito sia delle aziende, sia delle amministrazioni, vi può essere la necessità di accogliere alcuni documenti sotto forma fisica per poi trasformarli e leggerli in elettronico e far proseguire il resto del percorso con tale modalità.

Un'altra piattaforma di servizio fondamentale è, come si intuisce, la piattaforma dei pagamenti. Le operazioni di pagamento si accompagnano a quasi tutti i tipi di operazioni che svolgiamo nella vita personale e di lavoro, come ad esempio la fruizione di servizi.

Si tratta di alcuni requisiti di base ai quali la caratteristica di Poste italiane aggiunge un'infrastruttura logistica con i corrispondenti sistemi di tracciamento. Il tracciamento degli oggetti in mobilità, ossia quando un oggetto si sposta da un punto all'altro, o anche in funzione statica di archiviazione, è uno degli ulteriori valori che lo sviluppo moderno presuppone siano nelle mani di soggetti che traguardano, per esprimersi con una terminologia attuale, la cosiddetta « Internet degli oggetti ».

Noi vogliamo sapere in ogni momento, con un dettaglio sempre più preciso, dove l'oggetto che abbiamo comprato, che è giunto o che abbiamo archiviato, sotto forma sia di oggetto fisico, sia di documento, si trova in un dato momento, costruendone sia una serie storica, sia una serie gestionale per i fabbisogni correnti.

È chiaro che queste piattaforme non possono vigere da sole, altrimenti ci troveremmo nel problema che spesso nell'attività quotidiana veniamo a osservare, quello della difficoltà di far sì che dati provenienti e operanti su una piattaforma siano leggibili o trasferibili su altre. Tali piattaforme di servizio devono operare in una logica di integrazione fra di loro, non possono dar luogo a riferimenti puramente verticali, altrimenti ciò inibirebbe, per esempio, la possibilità per il cliente di accedere nella forma che ritiene più rispondente alle funzionalità di servizio e avere luoghi sicuri dove i propri dati, i dati della propria azienda o della propria amministrazione siano conservati.

Nel documento, in verticale in verde sono rappresentati alcuni esempi di tipologie di servizio che possono trarre beneficio dai primi due strati più quello di integrazione, che sono rappresentati, come l'*e-government,* la salute, la telefonia mobile in versione moderna e via elencando. Trasversale a tutta la piramide, che poi si esplicita verso l'esterno con i concetti di *cloud computing* verso soggetti privati, affari e amministrazioni, è la sicurezza dei dati.

La sicurezza dei dati si fa strada e deve rappresentare la garanzia di un servizio che per sua natura è aperto. Il concetto di *open data* implica necessariamente il raf-

forzamento della sicurezza sotto il profilo della *privacy* dei dati stessi, nonché della qualità della trasmissione dei dati e del non accesso da parte di altri. Vedremo poi la necessità anche della conoscenza di chi richiede queste informazioni sotto forma di dati, nonché di chi le eroga.

Trovate illustrati nel documento alcuni esempi che avevo anticipato prima di piattaforme di servizio. Una per tutte è quella della comunicazione elettronica, su cui si può immaginare il valore aggiunto che viene costituito dall'integrazione di queste funzioni.

Lo trasferisco con un esempio. Tipicamente nel commercio elettronico, al di là dei temi di identificazione, di cui parleremo, si acquista in anticipo per poi ricevere un oggetto. Ciò pone, anche nella tradizionale cultura delle Poste, non solo italiane, ma di tutte quelle che si basano sulla equidistanza fra mittente e destinatario, un vantaggio tutto a carico di chi, in questo caso, si comporta da mittente. Il mittente viene pagato in anticipo nel commercio elettronico, per poi, a valle del processo logistico, soddisfare l'esigenza del destinatario. In questo caso l'acquirente del commercio elettronico riceve l'oggetto dopo averlo pagato e può correre alcuni rischi connessi con il recapito e con la qualità dell'oggetto stesso.

Immaginate che un'integrazione di piattaforme permette in logica *web*, informando naturalmente mittente e destinatario, di fornire evidenza a entrambi dell'avvenuto pagamento, che viene tenuto congelato finché non è indicata in tempo reale l'avvenuta consegna, proprio per permettere di aprire il pagamento verso il mittente.

Immaginate la stessa funzionalità tramite portalettere. Il portalettere, che oggi è equipaggiato con un dispositivo di tracciamento logistico, di lettura di codici, e che quindi legge il codice impresso sull'oggetto, sul farmaco o su altro, accetta una funzione di pagamento e, quindi, le transazioni di logistica, cioè di avvenuta consegna, e di pagamento vengono indirizzate nei sistemi centrali che hanno originato questo tipo di richiesta.

Passiamo ora al *cloud computing*, con cui ci avviciniamo al tema della sicurezza informatica delle reti. Il *cloud computing* nella propria accezione presenta tre caratteristiche fondamentali. Si tratta di un luogo in cui vengono affittate una capacità di memoria e una capacità di calcolo. In altre parole, si tratta di una parte di infrastruttura a cui chiunque, azienda o amministrazione, può accedere, senza necessariamente aver dovuto effettuare un investimento, che può essere anche oneroso, ma soprattutto potendo, nella logica di *cloud computing* come declinata nella proposta di Poste italiane, fruire di un'infrastruttura che abbia caratteristiche intrinseche di sicurezza che difficilmente un singolo soggetto imprenditoriale potrebbe mettere in campo, se non ricorrendo a un investimento molto forte.

Provo a esemplificare. Tutte le funzionalità svolte da Poste italiane in termini di gestione dei dati, ossia esecuzione delle transazioni e memoria dei dati attraverso l'elaborazione degli stessi tramite le capacità di calcolo, avvengono secondo i criteri internazionali di *business continuity* e di *disaster recovery*, così come, per esempio, per i servizi finanziari è previsto dai regolatori internazionali e nazionali, ossia da Banca d'Italia.

Difficilmente possiamo pensare che l'operatore su un piccolo sistema possa accedere a funzionalità che gli consenta la salvaguardia, la tutela dei dati e la ripresa del funzionamento nei casi di eventi calamitosi e accidentali, perché queste funzionalità di *business continuity* e di *disaster recovery* implicherebbero un investimento aggiuntivo duplicato per raddoppiare le proprie capacità e delocalizzato rispetto al luogo in cui vengono erogate.

Ricordo che l'eventualità, purtroppo non tanto remota, perché ogni tanto ne siamo stati oggetto anche nel nostro Paese, di terremoti che isolano le capacità informatiche delle reti di determinati luoghi prevede che il recupero, la salvaguardia e la tutela dei dati e il ripristino della continuità del servizio avvengano in luoghi che, proprio per caratteristiche geografiche, devono essere distanti alcune centi-

naia di chilometri da quello in cui sono precedentemente conservati i dati. In queste ipotesi si deve prendere atto che un terremoto o un disastro possa avvenire in una località e che l'altro centro in cui si devono custodire i dati, con la sua capacità elaborativa, debba essere sufficientemente distante per non risentire degli effetti dell'evento.

Tutto ciò può essere oggetto di un'infrastruttura come quella di Poste italiane, ma è sicuramente difficile che una delle milioni di piccole e medie aziende possa dotarsi della medesima funzionalità.

C'è poi il primo livello di *cloud computing* come piattaforme di servizio, e qui arriviamo alla comunicazione elettronica. Noi tutti sappiamo che navigare su Internet è l'esperienza più affascinante degli ultimi vent'anni, navigare aperti, in libertà. Sappiamo altrettanto che le informazioni devono avere caratteristiche di riservatezza se a esse sono associate transazioni economiche particolari o, ancora di più, al punto alto del livello, si parla di servizi di *e-government*, tutti i presupposti di sicurezza sulla comunicazione elettronica devono offrire più di quanto non sia disponibile sull'Internet libera, quella che utilizziamo tutti i giorni.

Ancora, a un terzo livello superiore, quando si entra nelle piattaforme applicative di servizio, sempre per corredare il caso con un esempio, non necessariamente un'azienda che ha una propria missione di lavoro nel campo scelto dall'imprenditore deve dotarsi, nel concetto di *cloud computing*, degli applicativi di servizio che servono per eseguire la contabilità industriale. Tutti questi tipi di funzionalità possono avvenire in logica *cloud*.

Ritengo che sia una prospettiva assolutamente moderna quella di porre risorse a fattor comune di tanti soggetti e che essa imprima veramente un impulso e una possibilità di sviluppo a un tessuto imprenditoriale, ma anche amministrativo. Penso sempre alle piccole realtà, come tanti comuni, come la maggior parte dei comuni italiani, che ancora oggi non sono dotati di una cartografia digitale e che non hanno, quindi, in una memoria aggiornata e facilmente estraibile la mappa del proprio territorio, descritta con vie, numeri civici e natura delle abitazioni.

Questo è stato uno dei motivi per cui Poste italiane, avendo la cartografia digitale di tutto il territorio nazionale, ha potuto collaborare costruttivamente in quest'ultima edizione del censimento, proprio perché il presupposto della descrizione dei luoghi, della toponomastica e della natura delle abitazioni, distinte fra abitazioni, uffici e amministrazioni, è patrimonio corrente dell'azienda.

Dopo avere illustrato gli aspetti positivi del *cloud computing*, sicuramente il passaggio successivo sul quale ritengo che si debba investire e cimentarsi sono le piattaforme di servizio e gli applicativi; con la cautela che dobbiamo mettere in campo in termini di sicurezza.

Per cominciare, in questa sintesi la complessità e la vulnerabilità della rete, anche nell'accezione di ciascuno di noi nell'uso quasi quotidiano, quale che sia la finalità che ci proponiamo, è evidente. A volte ci troviamo a scaricare dati in maniera non chiarissima, magari veniamo attratti da apparenti offerte interessanti sotto il profilo economico.

Possiamo imbatterci, e capita tutti i giorni, in una rappresentazione di Poste italiane, se siamo sul sito di Poste italiane, che apparentemente è coincidente con quella di Poste italiane. Solo i più attenti, andando a verificare l'indirizzo IP, quello che si trova in alto nella schermata, si accorgono, però, che non è proprio uguale. Ciò significa che sono in corso fenomeni che mirano a catturare l'identità informatica delle persone e alcune informazioni essenziali.

Un altro fenomeno che si manifesta sul *web* è il cosiddetto attacco multiplo. Che cosa succede ? Sempre operando in una navigazione apparentemente interessante sul *web* ed effettuando collegamenti su siti di un'agenzia di viaggi, di un'offerta promozionale o di uno spettacolo, per anomalie registrate e individuate nel *software* applicativo del quale facciamo uso in quel momento, veniamo, in quella fase, clonati.

In altre parole, e mi piacerebbe avere l'occasione di potervelo mostrare in una dimostrazione reale, sulla *consolle* del clonatore compare e viene catturato l'indirizzo IP del computer dell'ignaro utente, che continua a navigare apparentemente in modo normale, ma il cui computer è ora guidato da un altro soggetto. In questo sta il concetto di attacco multiplo, che porta a esistere in questo momento, mentre parliamo, numerosi reti, cosiddette, nella terminologia, *botnet*, una contrazione per *robotnet*, che hanno affiliati a sé e governano fino a milioni di computer, dei quali si avvalgono per rivolgere e scatenare attacchi.

Di che natura sono tali attacchi ? Si trovano tutte le casistiche, da attacchi di natura dimostrativa fino ad arrivare alla scala più forte, attacchi di natura terroristica e rivolti contro gli Stati. Questi attacchi possono avvenire contro le infrastrutture in generale.

Devo operare una premessa, che forse non è sempre nota ai non addetti ai lavori. Con l'avvento di Internet si è diffuso sempre di più un protocollo di trasmissione che permette ai dati di essere trasmessi da qualsiasi parte e destinati a qualsiasi altra parte, chiamato proprio protocollo IP. Esso è stato successivamente, proprio per la sua semplicità e la sua efficacia, adottato in un grandissimo numero di situazioni, non tanto e non solo nelle reti di telecomunicazione, quanto anche in qualsiasi altro operatore faccia impiego di trasmissione verso punti periferici o raccolta di dati da punti periferici.

In altre parole il governo delle centrali elettriche si svolge nella stragrande maggioranza dei casi attraverso questo protocollo. Intuite, quindi, facilmente che l'interconnessione, e questo è l'aspetto positivo, è possibile nella maniera più ampia. Da qualsiasi computer, in qualsiasi parte del mondo, si può entrare, proprio per il fatto di parlare un linguaggio comune, anche nelle infrastrutture più riservate, apparentemente non solo di telecomunicazioni. Ne deriva il rischio di attacchi multipli alle infrastrutture.

Questi attacchi come possono essere condotti ? Essi possono avvenire, per esempio, nella forma cosiddetta di *denial of service*. Immaginate se a una qualsiasi funzionalità, per esempio in un sito di *e-government* in cui vengono fornite informazioni su servizi o in cui si erogano servizi, si inviino contemporaneamente tramite, queste reti di robot eteroguidate, milioni di *e-mail* di *spamming*, cioè milioni di *e-mail* replicate con la frequenza con cui possono essere mandate in rete, dell'ordine dei millisecondi. Nessun sistema è in grado di rispondere e, quindi, cade, perché bloccato. Se ne inibisce, dunque, l'accesso.

Formule di questo tipo e altre più sofisticate sono state utilizzate in ambiti di guerra elettronica, bloccando alcuni Paesi che risultavano, anche a livello europeo, esempi di modernità, proprio perché l'infrastruttura *web*, per quanto riguardava il funzionamento sia degli uffici governativi, sia delle principali aziende, si svolgeva in questa fattispecie. L'Estonia è rimasta bloccata per due settimane nei suoi funzionamenti essenziali. Il livello massimo del rischio è, dunque, un rischio Paese.

Ci sono anche formule molto più insidiose, non di questa portata devastante, ma che ci toccano come persone e anche nel mondo del lavoro sotto profili più mirati, che passano attraverso il furto dell'identità, in via preliminare, e che si sostanziano nell'attuazione di operazioni effettuate apparentemente in nome e per conto nostro. Esse ci portano disagi in termini sia di riconoscimento, sia, a volte, economici.

Quali sono le modalità con cui si muove prevalentemente chi opera in questo senso negativo sulla rete e quali sono gli strumenti di cui si avvale ? Un altro tipico esempio è quello dei *social network*. Nei *social network*, al di là, in genere, della presentazione individuale non sempre rispondente alla vera identità, ma a una presentazione di fantasia che ciascuno di noi ritiene istintivamente di porre come filtro nel proprio riconoscimento sul *web*, lo studio e la natura delle informazioni, nonché l'enorme numero di informazioni che girano è a sua volta una fonte che viene utilizzata altrove in momenti successivi.

Quali sono gli obiettivi e i bersagli di queste finalità ? Come abbiamo accennato, il primo è il furto di identità. La situazione più classica, la prima funzionalità di uso che si è determinata, è quella del commercio elettronico, del pagamento di oggetti o di acquisti effettuati *online*. Il primo punto di attenzione è stato quello di rubare l'identità per poi inserirsi nel mondo delle transazioni economiche.

Provo a rivolgere a voi una riflessione che stavo svolgendo per conto mio. Noi tutti abbiamo familiarità con il mondo dei sistemi di pagamento. Nel mondo dei sistemi di pagamento noi abbiamo una carta, alla quale è associato in maniera più o meno vincolante un codice.

Addirittura ci sono strumenti d'uso aggiuntivi. Quando ci inseriamo in un circuito finanziario, tipicamente ciò significa che facciamo leggere la nostra carta a un abilitatore. In ciò troviamo una coerenza interna in termini di sicurezza, che è una scelta anche di natura commerciale della pratica d'uso.

Se ci fate caso, perché con una carta di credito, alla cui transazione è annesso un maggior valore, in genere non è aggiunto un PIN di identità ? In altre parole, quando noi utilizziamo la carta di credito, la carta di credito viene strisciata e domani sarà inserita e letta in un microprocessore, ma in genere non ci viene chiesto di rafforzare la lettura della carta con un PIN personale.

Diverso è il discorso sulla carta di debito. Oggi addirittura sulla carta di debito e sulla carta prepagata, oltre alla lettura del PIN, si aggiungono anche altri tipi di funzionalità. Si tratta di un sistema che io definisco coerente in se stesso e che ha compiuto alcune scelte anche di natura commerciale, intendendosi, con il fatto di lasciare la carta di credito più libera rispetto all'altro tipo di carta, che ci si faccia carico dei rischi insiti nell'eventuale possibilità di frode.

Tutto ciò può essere visto in maniera dinamica e può cambiare. Però poi che cosa succede ? Quando noi andiamo a utilizzare questi strumenti nel mondo del *web*, i conti non tornano più, perché il proprietario della carta di credito che opera nel *web* non è necessariamente l'intestatario originario. Quindi, qualsiasi sottrazione di identità dal *web* non viene riconosciuta. Al *web*, infatti, interessa che il venditore venga pagato con una transazione che funzioni, ma non importa conoscere se colui che sul *web* si presenta con quelle credenziali sia la persona proprietaria o originaria delle credenziali medesime. Probabilmente non ne riceve danno, almeno nell'esempio che riporto, la parte venditrice, ma l'acquirente è sicuramente scoperto da qualsiasi tipo di difesa.

Poniamo per un attimo l'attenzione alla coerenza dei sistemi che al proprio interno hanno assunto nel tempo alcune cautele in termini di sicurezza e di protezione dell'identità, ma quando vengono utilizzate su un altro strumento o sul *web*, non offrono più lo stesso tipo di garanzie.

Vedete nel documento come, nella scaletta crescente, ai danni del singolo e dell'azienda si arrivi poi alle attività più critiche, che sono appannaggio degli organismi strutturalmente tenuti alla difesa. Sappiamo tutti che due o tre anni fa, non ricordo bene, negli Stati Uniti è stato riconosciuto al Cyber Command un rango di forza armata, cioè si è assegnata a questo tipo di operatività sul *web* una natura militare.

Evidentemente questo è il caso più estremo e io non andrò a trattarlo, ma mi soffermerò sugli aspetti che nella vita corrente, privata e di lavoro, possono maggiormente essere oggetto di attenzione e di provvedimenti.

Alcune questioni che già vi ho illustrato sono tratte da dati statistici piuttosto recenti. Tornando al fenomeno delle *botnet*, ce ne sono sette principali. Ciascuna raggruppa centinaia di migliaia, se non addirittura milioni di computer, come la Zeus. Noi siamo il terzo Paese più attaccato. Ho preso alcuni dati statistici per suggerire il senso e la dimensione del fenomeno.

Un altro fenomeno caratteristico è quello degli attacchi agli archivi aziendali, perché in una volta sola, come si intuisce, si raccoglie un numero di informazioni di

gran lunga superiore a quello del dover seguire momento per momento tanti singoli clienti, approfittando di un loro attimo di distrazione o di un fenomeno cosiddetto di *phishing*, che rende l'idea del senso della cattura, per assumere le identità degli utenti. Questo fenomeno, mentre negli ultimi tre anni era andato a scemare, ha ripreso fortemente vigore.

Ritorno per un attimo al tema del *cloud computing*. Non c'è alcun dubbio, e io ne sono profondamente convinto, che l'evoluzione di un Paese possa trovare uno strumento utile l'erogazione di servizi in logica *cloud*, ma è altrettanto vero che, in maniera ancora più stringente, la difesa degli archivi dove sono conservati i dati è un elemento che richiede estrema attenzione e cautela.

Passando al caso dei singoli, vi è il furto di identità, su cui sono stati messi in evidenza alcuni casi: ci sono 1,5 milioni di carte di credito Visa e Mastercard le cui identità sono state rubate, cui si aggiunge il furto a danno della Sony e via elencando.

Vediamo quali sono state le nostre iniziative. Tanto per cominciare noi ci siamo accorti sul campo che, mano a mano che si diffondeva l'uso delle carte prepagate di Poste italiane – non vuole essere una nota di *marketing*, ma oggi ne circolano poco meno di 9 milioni –, l'attenzione del *web* passava su di esse.

La carta prepagata è lo strumento più utilizzato per gli acquisti di commercio elettronico. Ciò avviene perché istintivamente l'acquirente non ha fiducia nel dichiarare i dati della propria carta di credito, che, per definizione, implica un importo potenziale più elevato a cui attingere, ma ritiene che ci sia una minore rischiosità quella di poter destinare a tale finalità uno strumento che, essendo per sua natura una moneta elettronica, è destinato a contenere cifre significativamente più modeste. Si tratta di una giusta reazione istintiva.

Noi abbiamo cominciato a vedere che l'attenzione del mondo *web*, quella impropria, era passata dalle carte di credito alle carte di debito, fino ad arrivare alle carte prepagate. Abbiamo cominciato allora a reagire a tutto campo, sia dotandoci di strumenti, sia cercando, vista la globalità della fenomenologia, di trovare alcuni *partner* con cui operare che avessero specifiche competenze, ponendo in essere alcune iniziative.

Quali sono le iniziative ? Le pongo in ordine logico, anche se temporalmente non sono state realizzate proprio in questo modo. In primo luogo abbiamo costituito una fondazione di carattere internazionale, perché ci siamo accorti che nell'uso corrente e soprattutto nella naturale difesa dell'utilizzatore, di colui che effettua le transazioni e le operazioni finanziarie su *Internet*, non c'era un profilo di regole internazionali che potesse garantire immediati interscambi nel *web* atti a garantire l'interessato.

Che cosa significa tutto ciò ? Ancora oggi nella nostra sala di controllo per la parte informatica noi verifichiamo dai dieci ai venti attacchi di cosiddetto *phishing* al giorno. Sono attacchi che si propongono e attuano sul *web* attraverso siti sempre più simili a quello di Poste italiane. All'interno di questi siti si listano alcune domande, che non sono pertinenti, ma che frequentemente possono trovare persone che istintivamente rispondono. Ciò significa acquisire informazioni e rappresenta il presupposto o l'atto con cui viene rubata l'identità.

Che cosa si fa con il furto di identità ? Da dove vengono questi attacchi di *phishing* ? Sto parlando del caso più semplice. Gli attacchi di *phishing* vengono da *server* di cui viene tracciato l'indirizzo Internet, che sono in qualsiasi parte del mondo. Sono veramente questi *server* il luogo origine dell'attacco ? Non necessariamente, perché a sua volta un *server* può essere stato violato e, quindi, il proprietario del medesimo è ignaro del fatto che il suo *server* sia stato controllato e violato da altri.

In altri termini, ci è capitato anche recentemente di rispondere ad alcuni attacchi che venivano da una sede universitaria negli Stati Uniti, la quale era ignara del fatto che il proprio *server* fosse stato compromesso e che da esso partisse un attacco verso Poste italiane.

Che cosa ci fa intuire ciò? Più tempo rimane aperto un sito clone di Poste italiane o di un altro soggetto e maggiore è la probabilità che un ignaro utilizzatore, ritenendolo vero, interagisca nel sito e fornisca informazioni che non dovrebbe fornire.

Sorge immediato il tema di come si fa a operare a livello internazionale per chiudere immediatamente queste funzionalità, che sono segnatamente false. Non sfugge che ancora oggi regole globali di interscambio fra i Governi e le forze di polizia non sono in atto. Esistono magari accordi bilaterali o trilaterali, buone pratiche di collaborazione, ma non esiste un *framework* di regole che sotto questo profilo – ho portato l'esempio forse più semplice ed evidente – tuteli il cliente che accede a *Internet*.

Perché abbiamo costituito la fondazione? Proprio la globalità di Internet implicava il fatto che competenze di natura diversa e apparentemente separate, in questo ambito dovessero trovare il modo di lavorare insieme. Stiamo parlando di competenze giuridico-legali, di competenze di tipo regolatorio e poi, « scendendo per li rami », di competenze e di compiti degli operatori di servizio.

Si affaccia, a questo punto, un tema, a mio avviso, fortissimo: che cosa i Governi, le istituzioni e i regolatori devono pretendere dagli operatori di servizio, coloro che offrono i servizi al cliente?

Si scende ancora fino al momento delle industrie specializzate, sia nei settori di informatica e telecomunicazioni, sia nell'ambito degli algoritmi e delle criptazioni, per arrivare alle università e ai centri di ricerca.

Questa fondazione sta operando ormai dal 2010. Vedete i loghi di alcuni degli aderenti. Si intuisce come alcuni dei principali aderenti rispondano proprio a questo aspetto di multidisciplinarietà, secondo il tentativo, spesso coronato da positività, di mettere a frutto in maniera integrata le proprie competenze.

Vi è uno studio recente che stiamo svolgendo. Come sapete, tutti i domini del mondo sono rilasciati da un'azienda di diritto statunitense che si chiama ICANN, che agisce secondo una serie di protocolli in una catena gerarchica. È altrettanto vero che il cosiddetto *domain name system*, cioè l'assegnazione del nome dei domini, che è quello che contraddistingue, accoppiato alle altre caratteristiche del cliente, la possibilità univoca di essere identificati, viaggia senza avere algoritmi di protezione, quali possono essere quelli che, nell'accezione normale, noi identifichiamo con la firma digitale, ovvero con la separazione di due chiavi, una pubblica e una privata, la cui combinazione, almeno fino a oggi, riesce a offrire le garanzie di riservatezza necessaria.

Che cosa significa tutto ciò? Sin dal livello dell'assegnazione dei domini, nella funzionalità dei *server* che in tutto il mondo interagiscono fra di loro, è latente il rischio di una rottura, di una penetrazione negli indirizzi. È un rischio di portata elevata, al quale la fondazione sta collaborando, provando a diffondere le caratteristiche di un *domain name system* sicuro, il che comporta introdurre nei nuovi *server* le modalità di funzionamento con algoritmi di tipo firma digitale.

Un ramo della fondazione è la European Electronic Crime Task Force. A livello ancora più operativo, i soggetti sono sempre di natura interdisciplinare, ma va da sé che le forze di polizia, in questo caso, sono l'elemento motore più attivo, sia nel raccogliere dagli operatori le informazioni che possono portare all'identificazione e alla soluzione dei fenomeni criminosi, sia, a loro volta, nel fornire agli operatori gli elementi di cautela che servono per prevenire queste finalità di aggressione. Se ci fosse interesse, potrei illustrare alcune caratteristiche della fondazione.

C'è poi un terzo punto che, a mio avviso, merita un'attenzione e una riflessione ancora più generale. Nel mondo degli operatori postali anche centocinquant'anni fa – ritorno al passato soltanto per rendere, spero, meno monotona l'esposizione – il concetto di comunicazione veniva declinato in termini di riservatezza. Addirittura abbiamo esibito alla

nostra mostra itinerante, che adesso è a Roma, un giuramento di riservatezza che prestavano gli ufficiali postali nella seconda metà dell'Ottocento. Evidentemente la natura della comunicazione poteva essere facilmente divulgata aprendo un oggetto fisico ed era facile, leggendone il contenuto, farne usi non propri, così come nella trasmissione telegrafica.

Se ci riflettiamo, la trasmissione telegrafica rappresenta il primo esempio di trasmissione dati criptata della storia. Il codice non era difficilissimo, ma era comunque una barriera all'ingresso sia per chi doveva trasmettere, sia per chi poteva ricevere. Era un elemento tecnologico in più.

Tornando ad oggi, il mondo degli operatori postali in comunicazione elettronica sul *web* presenterà nella prossima riunione plenaria che si terrà il prossimo mese di ottobre in Qatar il dominio « .post », un dominio di primo livello che garantisce l'interoperabilità fra tutti gli operatori postali del mondo che aderiranno al medesimo e che traguarda la sicurezza della comunicazione fra qualsiasi soggetto, qualsiasi siano il mittente e il destinatario, garantendo tutte le caratteristiche ormai familiari nell'uso della posta elettronica, ma con un'identificazione certa e forte del soggetto mittente e del soggetto destinatario e una protezione della trasmissione da intrusioni sul *web*.

Strumenti come la marca elettronica o la firma digitale garantiscono l'uno l'integrità del documento su Internet, ossia che il *file* che siamo usi trasmettere da un punto all'altro non sia stato aperto da alcuno, e l'altro che il mittente sia proprio quello che è stato identificato fortemente e la cui identità elettronica è autorizzata a viaggiare sul *web*.

Poste italiane in questo senso ha l'incarico di sviluppare tutti i servizi di comunicazione elettronica per il « .post ». È un punto importante, in cui l'univocità, l'interoperabilità e la garanzia della comunicazione elettronica sicura avvengono a livello di agenzia dell'UPU che unisce tutti gli operatori postali del mondo.

Andiamo a vedere nella pratica qual è la nostra opinione per un *provider* che deve garantire i propri clienti nella funzionalità continua nel mondo *web*.

Prima di tutto abbiamo visto che c'è una funzione di monitoraggio indispensabile. Dagli esempi che vi portavo prima si intuisce che non si debba aspettare il momento in cui avviene l'eventuale frode di sostituzione di persona o monetaria per intervenire. Il preliminare necessario è un monitoraggio continuo del *web*, perché nel monitoraggio continuo del *web* in fase anticipata si registrano gli eventi che poi successivamente possono dar luogo alla vera e propria effrazione.

Che cosa significa tutto ciò ? Eventi apparentemente coerenti singolarmente, se correlati insieme da metodologie e analisi di rischio, portano a evidenziare in maniera preventiva se c'è nel *web* un'azione o un'iniziativa che prova a catturare l'identità elettronica del malcapitato.

Come si vede ciò ? Si vede, per esempio, correlando alcuni indirizzi IP e osservando se, a distanza di poco tempo, il collegamento di quelle macchine avviene non soltanto dalla stessa località, ma anche da diverse parti del mondo.

Si attua, ancora, analizzando i sistemi operativi. Se si ha un proprio cliente al quale, per esempio, è annesso il naturale impiego di un computer, di una macchina con un sistema operativo in italiano, trovarlo in rumeno o in cinese è un indice sospetto e via elencando.

Si vengono, pertanto, a correlare alcuni elementi che ancora non sono l'evidenza della frode, ma sono l'indice o che un malcapitato è stato clonato o che su di esso si sta concentrando un'attenzione per carpirne l'identità.

Dopodiché, dopo la fase del monitoraggio si sostanzia quella dell'analisi, che passa attraverso algoritmi di correlazione, i quali pongono in essere operazioni apparentemente distanti fra di loro, ma correlabili soltanto attraverso un'analisi sofisticata di passaggi.

Infine, si arriva alla vera e propria operazione di contrasto e, quindi, al con-

cetto di come si definisce l'identità elettronica, come la si deve mantenere e come la si deve misurare.

PRESIDENTE. Ricordo ai colleghi che – penso che questo sia l'ultimo capitolo e che in cinque minuti l'ingegnere terminerà – i lavori dell'Aula iniziano a mezzogiorno, ma che le votazioni si svolgeranno dopo le 13,15. L'ingegnere ha dato la disponibilità per rimanere fino alle 13, perché c'è una seconda audizione, cui so che molti colleghi sono interessati e che deve essere tenuta distinta da questa, essendo anche da un punto di vista regolamentare diversa.

SILVIA VELO. Vorrei intervenire sull'ordine dei lavori. L'amministratore delegato, con una relazione molto interessante, si è comunque preso due terzi del tempo che avevamo per questa prima parte. Forse alcuni colleghi hanno la necessità di andare in Aula; si parla della possibilità che oggi il Governo ponga la questione di fiducia; l'audizione che segue è informale. Se non riuscissimo a concludere la parte successiva, domani potremmo ricalendarizzare il prosieguo.

PRESIDENTE. Chiedo all'ingegnere se sia possibile.

MASSIMO SARMI, *Amministratore delegato di Poste Italiane Spa*. Sicuramente, presidente. Arrivo alla conclusione e ringrazio il presidente per la pausa che valorizza quello che credo sia il punto più importante e centrale di tutto ciò che abbiamo illustrato. Il primo tema è la necessità di operare e offrire servizi in logica *cloud*, il secondo l'uso sempre più corrente del *web* con tutte le sue opportunità, ma anche con i rischi connessi, e il terzo il fatto che la navigazione sul *web*, quale che ne sia il motivo, deve far perno su un'identità digitale.

Che cosa andiamo a vedere ? A livello internazionale il tema è di grandissima attualità, ma non esistono norme internazionali di ampio spettro che affrontino la questione dell'identità digitale.

Ci sono alcuni *standard* tecnici di tipo molto ampio, come l'ISO, oppure c'è la volontà da parte di alcuni grandi operatori del *web* – leggasi e-Bay, Google o Facebook – di proporre alcuni standard *de facto*. Sicuramente, in questi casi, però, si tratta di una finalità di natura commerciale, mentre il tema dell'identità digitale è molto più ampio.

Passando dall'ambito internazionale all'ambito nazionale, anche in quest'ultimo non esistono norme che regolino l'identità digitale. Ci sono alcune specificità che riguardano più il diritto alla *privacy* e la protezione dei diritti dell'individuo.

Secondo me, ci sono due percorsi. Uno va verso un mondo di fruizione di servizi di natura tipicamente commerciale, come l'acquisto di un servizio o di un oggetto sul *web*. Come ci si muove in tale ambito ?

Sommariamente, un operatore di servizi che ha a disposizione le informazioni di comportamento dei suoi clienti ricorrenti può sia utilizzare l'aspetto tecnologico, sia conferire a esso un peso di rischio commerciale tale da farsi carico di riconoscere l'identità del proprio cliente proprio in funzione dei profili di uso. È come se immaginassimo un *customer relationship management*, lo strumento cuore per la conoscenza dei clienti, che ne analizza in tempo reale le fruizioni d'uso sul *web* e garantisce o non garantisce di essere proprio lui il *provider* del servizio tramite i propri comportamenti.

Il soggetto che opera in natura commerciale può dar credito a tale propria valutazione e non richiedere, quindi, al cliente identificazioni all'ingresso del servizio più o meno forti, da un lato portandosi a casa una semplicità di dialogo con il cliente stesso e, dall'altro, accettando un rischio di dimensione contenuta, rendendosi pronto ad alzare le barriere nella misura in cui vedesse che tale rischio viene elevato.

A mio avviso, non può ragionare in tal modo, invece, la pubblica amministrazione. La pubblica amministrazione non può, a mio avviso, correre il rischio di dialogare sul *web* con dati di natura riservata, quali che essi siano, per poi an-

dare nel profilo dei servizi più evoluti senza avere riconosciuto con un'identità forte il soggetto che si sta presentando.

Secondo me, pensare a una diffusione di servizi di *e-government* presuppone l'aver trattato e risolto questo tema, che è importantissimo. Non voglio esprimermi in termini negativi, ma pensate a che cosa succederebbe se io diventassi il richiedente e acquisissi importanti dati sensibili che, in realtà, sono di un altro, nell'ambito della salute, nel processo telematico o in qualsiasi altra funzionalità in cui l'identità elettronica deve essere pienamente corrispondente a quella fisica.

La strada può essere di due indici, uno più di natura commerciale, con tutte le cautele che si può imporre il soggetto erogatore del servizio, e un altro che, secondo me, deve distinguere tutto ciò che avviene fra amministrazioni cittadine e fra cittadini e amministrazioni.

Che cosa occorre fare? Occorre definire alcuni standard di identità digitale e di interoperabilità e poi, e in ciò c'è anche un ruolo di Poste italiane, quali sono le regole di ingaggio del *service provider*. Gli scenari sono due: nel primo è solo l'amministrazione dello Stato a farsi carico della gestione dell'identità digitale con infrastrutture, mezzi e tutto ciò che è necessario, nel secondo si pensa di delegare le funzioni di riconoscimento in parte anche ad alcuni *service provider*.

In questo secondo caso servono alcune regole. Il sistema regolatorio, a mio avviso, deve occuparsi di queste, così come di definire regole di funzionamento di controllo, di livelli di servizio e soprattutto della possibilità di federazione dell'identità nazionale in ambito internazionale.

Fino ad oggi, mentre vi ho citato l'esempio dell'Unione postale universale, che assume uno standard di interoperabilità di valenza mondiale, va da sé che, anche in un ambito di Unione europea, con funzionalità di scambio che già oggi si presume saranno fortemente crescenti, che la federazione delle identità stabilite in ambito nazionale sia un tema della massima importanza.

Passiamo all'ultima *slide*. Il grafico indica sull'asse delle ordinate come ci si registra e su quello delle ascisse i livelli di sicurezza che si vanno a sostanziare.

Se andiamo a vedere, non in tutto il mondo ma in molti Stati, gli strumenti tradizionali che garantiscano, in fase sia di registrazione sia di riconoscimento, l'identità elettronica in maniera coerente, notiamo che lo strumento che conosciamo è il passaporto elettronico. Nel rilascio c'è l'identificazione a vista, con l'associazione di dati biometrici, mentre nell'utilizzo, non in tutto il mondo, ma in molti Paesi, c'è un procedimento contrario, che è assolutamente analogo: c'è il riconoscimento a vista, accompagnato dall'analisi biometrica e dall'interrogazione delle banche dati.

Come accennavo prima, occorre trasformare sul *web* quest'identità forte a livello sia di registrazione, sia di autenticazione. A livello di registrazione non può esserci altro modo che l'identificazione fisica del soggetto prima dell'ingresso; nel mondo *web*, per le finalità che abbiamo descritto, non può non esserci un'identificazione fisica. Vediamo alcuni esempi.

A parte il passaporto, c'è un'indicazione forte tipicamente nelle aziende, ma anche nelle amministrazioni, quando ci rilasciano il tesserino di riconoscimento che ci permette l'accesso o l'ingresso. Addirittura non solo c'è l'identificazione fisica, ma ci vengono richiesti anche documenti – ricordo la circostanza di quando sono stato assunto in azienda – quali il casellario giudiziale e numerosi altri elementi importanti.

Sul *web*, però, non siamo in queste condizioni. Come possiamo muoverci nel mondo del *web*? Tanto per cominciare la registrazione non può che avvenire con un elemento di fisicità, o con l'amministrazione direttamente, per il tramite di soggetti che fanno parte dell'amministrazione stessa, o per il tramite di un *provider*, così come capita con Poste italiane, quando identifichiamo fisicamente le persone. Segue un viaggio attraverso il *web*, che deve essere garantito nella maniera opportuna, dal monitoraggio, alla

decisione e alla gestione. Infine, ci sono l'identificazione e l'uso di strumenti che rafforzano il viaggio *web*.

Oggi, seppure in una normativa ancora non consolidata, si distinguono tre tipi di autenticazione: un fattore, come un PIN, che può essere più o meno forte a seconda del numero dei caratteri; si aggiunge al PIN il possesso di una *smart card*, cui può essere abbinato, per creare una combinazione tramite un algoritmo di criptazione, un valore combinato; o ancora un terzo fattore aggiunto, che può essere quello del riconoscimento biometrico. La considerazione finale non ha la pretesa di essere un'indicazione cogente, ma sicuramente un elemento di forte riflessione.

Provo a portarvi un esempio di vita corrente. Alle carte prepagate Postepay non associavamo in passato alcun PIN. Ora abbiamo aggiunto un PIN. Alle transazioni più importanti aggiungiamo anche una generazione, ossia la combinazione fra un PIN, il codice, e una generazione di un numero casuale abbinata al PIN. Stiamo, inoltre, per aggiungere l'abbinamento di un numero casuale generato dalla transazione. Esistono già alcune modalità sul *web* per catturare, durante una sessione, l'identità elettronica degli interessati. C'è un'evoluzione continua.

Sono arrivato alla conclusione. Chiedo scusa per il tempo che ho impiegato per la relazione. Sono pronto a tornare in seguito, come chiedeva il presidente, in momenti successivi. Credo che questo sia un punto, quello del *cloud computing* e dell'identità elettronica, per esprimersi in termini di sintesi, che in un profilo di agenda digitale emerge come uno dei punti di maggiore importanza per il profilo di sviluppo dell'uso del *web* e di tutti i servizi a esso correlati.

PRESIDENTE. Grazie, ingegner Sarmi.

Do la parola ai deputati che intendano intervenire per porre quesiti o formulare osservazioni.

CARLO MONAI. Ringrazio l'ingegner Sarmi per la sua relazione, molto tecnica, ma anche suggestiva e densa di spunti. Pensavo come anche alla Camera dei deputati ci siamo posti il problema della registrazione e dell'autenticazione, tanto che abbiamo introdotto le minuzie per identificare i deputati chiamati al voto. Forse questa potrebbe essere un'indicazione di sicurezza particolarmente pregnante, perché assocerebbe alla facilità dell'identificazione da parte dell'utente una quasi assoluta certezza dell'identità dell'operatore.

Ciò porterebbe alla necessaria evoluzione anche dell'*hardware,* alla vendita di supporti già incorporati nei computer e via elencando. Al di là di codici numerici casuali o che l'utente deve ricordare e che possono essere sempre copiati nell'evoluzione virtuale di una guerra tra guardie e ladri, che in questo contesto diventa molto più evanescente, visto che il linguaggio degli operatori è universale, rilevo che non è altrettanto universale la capacità delle guardie di ergersi a difesa di questo mondo delle comunicazioni. È, invece, più facile per i ladri riuscire a inerpicarsi su sentieri sempre meno conosciuti e visibili.

Uno dei temi che volevo sottoporle è la prospettiva che ho visto, da voi sostenuta, di questa fondazione, la quale, peraltro, dovrebbe avere e penso che abbia una valenza internazionale, sia pure realizzata in Italia. Penso che ciò sia merito vostro e che la fondazione debba necessariamente cercare di accelerare quanto prima una rete di sicurezza internazionale, che vedo essere stata avviata a livello europeo, ma con l'aiuto degli Stati Uniti, se ho capito bene. È stato stipulato un accordo tra Ministero dell'interno e forze di sicurezza statunitensi nel tentativo di dotare l'Europa di un sistema di sicurezza proprio, che penso si aggiunga a quello già adottato in altri continenti. Questa è una prima domanda.

Il traguardo è quello di una tutela globale che ovviamente pone anche problemi di tutela della *privacy* e di schedatura dei soggetti che entrano in contatto con la rete, ma io penso che il tema della sicurezza sia più importante di quello della *privacy,* nella misura in cui a ciascuno di noi è capitato nell'esperienza quotidiana di essere vittima di piccole

truffe o di piccole o grandi ruberie da parte di operatori che si presentano come affidabili e poi magari nascondono le identità più diverse, riuscendo ad accaparrarsi denaro o altre utilità.

Venendo al tema della Polizia postale, so che è in corso un contratto triennale tra Poste italiane e Ministero dell'interno che dovrebbe scadere a dicembre del 2013. Si tratta di 2.000 funzionari di Polizia postale, che hanno ospitalità nelle vostre sedi e che da quelle località riescono a esaudire indagini investigative loro proprie, nonché delegate dalla diverse procure, a cui fanno riferimento tutti gli uffici di Polizia giudiziaria. Anche Guardia di finanza, Carabinieri e questure hanno nella Polizia postale la testa d'ariete specializzata nella lotta alla criminalità elettronica.

Mi è stato paventato il rischio che questo contratto non verrà rinnovato perché comporta oneri piuttosto importanti a carico, se ho capito bene, di Poste italiane. Mi offre rassicurazioni in questo senso ? Se esiste effettivamente questa prospettiva, come potremmo noi deputati attivarci per evitare che questo patrimonio di conoscenze e di funzioni di polizia assolutamente importanti in un contesto quale quello attuale, che vede l'*e-commerce* sempre guadagnare posizioni rispetto alle attuali, non venga perso ? Sarebbe paradossale che, a fianco di queste vostre iniziative, tese a rendere più cogente ed efficace la lotta al crimine, si veda depauperare un patrimonio di professionalità che è attualmente importante e che penso debba essere potenziato e certamente non annichilito.

DEBORAH BERGAMINI. Grazie, ingegnere. Ho trovato interessante la sua relazione tecnica, ancora di più nel momento in cui questa Commissione si appresta a esaminare un testo unificato sull'agenda digitale per il nostro Paese. È evidente che questa relazione è il frutto – lei ha parlato di un'ampliata geografia di presenza di Poste – di un osservatorio sicuramente centrale nel sistema del nostro Paese anche da questo punto di vista.

È molto interessante un concreto rischio di paralisi del sistema delle comunicazioni elettroniche. Lei di fatto, spiegando quali e quanti sono i potenziali danni provocati dal crescente attacco dell'hackeraggio nei confronti dei sistemi della pubblica amministrazione – mi soffermo su questi – ha evidenziato come tale tema meriti una grande attenzione.

Raccolgo anche il tema legato a un rafforzamento del concetto di identità digitale, senza il quale è difficile riuscire a mettere a sistema un funzionamento alternativo a quello tradizionale per quanto riguarda il rapporto fra il cittadino e la pubblica amministrazione. Sicuramente sono indicazioni che coglieremo.

Proprio perché stiamo per affrontare il tema dell'Agenda digitale, le volevo chiedere qual è la sua posizione rispetto al famoso tema degli atti a riserva, ossia delle notifiche delle multe e degli atti giudiziari. Io credo che una forte efficienza si potrebbe raggiungere se si consentisse di notificare i provvedimenti anche attraverso la posta elettronica certificata e, quindi, le vorrei chiedere se lei sarebbe d'accordo col fatto di sollevare questa riserva e di aprirsi anche a quest'altra modalità, in modo tale da rendere più efficiente il mercato dei servizi postali e anche garantire un risparmio di risorse e di tempo, che è in primo luogo quanto interessa di più ai consumatori.

La seconda domanda, alla quale desidererei avere risposta, ma immagino che non le sarà possibile rispondere ora, riguarda i costi per il cittadino delle transazioni *online* per i servizi postali e non solo, ossia il perimetro di attività di Poste. Credo di non essere l'unico parlamentare a cui arrivano segnalazioni di costi troppo elevati per queste operazioni.

Non so se voi avete raccolto dei parametri europei nei Paesi comparabili ai nostri, se avete una media dei prezzi da voi richiesti rispetto ai vostri omologhi dei Paesi assimilabili al nostro. In tal caso mi farebbe piacere avere queste informazioni, perché è un tema sul quale sono molti i cittadini che si dichiarano insoddisfatti.

PRESIDENTE. Do la parola all'ingegner Sarmi per la replica, ringraziandolo anche

per la relazione, che comunque, anche se lunga, verte su un argomento molto delicato non solo dell'oggi, ma soprattutto del futuro.

MASSIMO SARMI, *Amministratore delegato di Poste Italiane Spa*. Grazie. Provo a rispondere rapidamente.

Innanzitutto il rapporto con la Polizia postale è un bel rapporto. È cominciato con uno scambio di attività di natura tradizionale e si è evoluto negli anni incentrando moltissimo la corresponsione e l'aspetto economico legato a questo contratto sulla parte elettronica. Il loro centro CNAIPIC è stato in parte anche finanziato con le risorse che provenivano dalla convenzione con Poste italiane.

C'è assolutamente il desiderio di continuare. Tutte le volte in cui si effettuano e si effettueranno negoziazioni si cerca di essere ognuno più attento agli interessi della propria azienda o dell'amministrazione, ma sicuramente è un percorso positivo virtuoso.

Ricordo che, quando parlavo prima di arrivare materialmente alla fondazione, sentimmo l'urgenza di costituire la *task force* sul crimine elettronico e i fondatori furono proprio la Polizia di Stato, il Secret Service americano e Poste italiane. Poi naturalmente il gruppo si è allargato.

Il fatto che parte delle alleanze originarie siano di tipo statunitense è comprensibile, perché tutto il mondo dell'elettronica e dell'ICT in generale oggi viene sviluppato in quella zona del mondo, né mi sento di affermare che le garanzie che vengono offerte da produzioni localizzate in altri Paesi in termini di trasparenza dei contenuti e di attenzione nei confronti della *privacy* siano altrettanto diffuse.

L'*imprinting* di natura europea si è fortemente sviluppato immediatamente dopo. Noi siamo costantemente in contatto con la ricerca e collaboriamo anche con i numerosi organismi che in ambito europeo, con delega specifica o su loro iniziativa, si stanno occupando di questa materia.

L'onorevole Monai ha affermato giustamente che il mondo del *web* è globale. Non pensiamo di limitarlo all'Italia o all'Europa, perché avremmo una visione veramente miope.

C'è un altro concetto banale, che trasferisco con un esempio. Quando anche a noi, un dato giorno, entrarono nel sito, compiendo un cosiddetto *defacement* – nella pagina del sito e non nei dati – alla fine, lavorando con la Polizia postale, ricostruimmo che gli autori erano tre soggetti, ciascuno dei quali non si era mai conosciuto prima d'ora. Uno era un figlio di buona famiglia, un altro era un soggetto sulla china della criminalità e il terzo un rumeno che si era trovato di passaggio e che aveva pensato di fare un affare. Prima che tre soggetti di tre amministrazioni mondiali si mettano insieme con la stessa rapidità trascorrerebbe molto più tempo. Ci dobbiamo porre questo tema, perché è cogente.

Ringrazio l'onorevole Bergamini per le sue parole. Sulla notifica, secondo me, noi dobbiamo evolvere in termini di posta certificata, corroborata da un percorso di identità elettronica forte. Parlare di posta elettronica certificata, se poi non garantiamo chi è il soggetto che dialoga con l'amministrazione e viceversa e non manteniamo questa garanzia, è inutile. Mantenere questa garanzia significa non solo e non tanto utilizzare strumenti e algoritmi, ma, come tengo a precisare, anche un sistema di monitoraggio di studio costante, perché il crimine informatico evolve costantemente. Se si vuole operare in quest'ambito come si deve, non possono che esserci dietro soggetti o pubblici o delegati dal pubblico che si muovono con regole speciali e con compiti specifici e precisi che continuamente offrano la garanzia di evolvere come evolvono gli strumenti di natura eterodossa.

Per quanto riguarda un aspetto di Poste italiane, le rappresento un esempio analogo. Ci stavamo interessando, sempre per motivi di interesse dell'azienda, dello sportello unico per le imprese. Perché lo sportello unico, pur essendo previsto, ha difficoltà a essere realizzato ? Le rispondo subito. Chiunque voglia aprire un esercizio commerciale deve chiedere un certificato a un'ASL o ai vigili del fuoco. Se noi pensiamo di aspettare che tutti questi orga-

nismi siano in rete nella maniera congrua, credo che le funzionalità sarebbero ritardate assai a lungo.

Il ruolo di Poste italiane è proprio quello di complementare le velocità, quella del puramente elettronico e quella dell'ibrido, come accennavo all'inizio – quando qualcuno produce un documento in fisico, esso viene letto otticamente e segue poi un percorso elettronico – che è quanto facciamo oggi per l'erogazione dei permessi di soggiorno.

Non dimentichiamo che in logica *cloud* tutto il sistema dei permessi di soggiorno, oltre 6 milioni, è gestito, in nome e per conto del Ministero dell'interno, da Poste italiane: accoglienza del cliente, riconoscimento forte a vista, accettazione di documenti scritti, trasformazione in elettronico, acquisizione di flussi di dati tipicamente dai patronati, congruenza interna, invio dei flussi al Poligrafico dello Stato.

Una volta trovate tutte le congruenze, segue l'integrazione con il sistema del Ministero dell'interno. La persona nella questura apre il suo schermo e vede che può chiamare l'interessato, in quanto tutto ciò che doveva essere risolto nella parte preliminare è disponibile e, quindi, può avvenire la consegna del permesso.

Anche in questo caso non sfugge che, a mio avviso, dobbiamo tener conto che questi sistemi dovranno essere necessariamente misti ancora per anni, ma dobbiamo anche trasformarli tutti, laddove la velocità di ingresso fosse quella del documento fisico, per esempio, alla velocità dell'elettronica, oppure viceversa. Abbiamo operato con il Ministero della giustizia per anni proprio sulle notifiche, andando di pari passo con l'evoluzione e con l'informatizzazione a livello di cancellerie.

Lei sa, onorevole, che, per dare consistenza a un'udienza, cioè per far sì che le persone che devono essere presenti lo siano effettivamente, deve esserci una notifica, seguita da un accertamento di notifica, altrimenti l'udienza non può aver luogo. Tutto ciò oggi avviene in complementarietà con un portalettere, il quale, nel momento in cui notifica l'atto nella versione tradizionale, invia un'informazione in elettronico. Se dall'altra parte c'è la possibilità di accogliere in elettronico, tutto si svolge in elettronico, altrimenti noi creiamo le immagini ottiche delle avvenute notifiche e le inviamo alle cancellerie.

Dobbiamo essere, a mio avviso, flessibili nel poter realizzare la finalità sia nell'accogliere in ingresso, sia nel distribuire in uscita tutto ciò che non può che avere sicuramente un cuore elettronico e nel progredire un'interezza del percorso in elettronico.

Mi aveva chiesto, infine, i prezzi dei servizi *online*. Li andrò a vedere. Per la verità, l'operazione più comune che noi effettuiamo è il bollettino. Forse in prospettiva ne diminuiremo il prezzo rispetto al mondo fisico. È altrettanto vero che proprio su questo, essendo un prodotto di mercato, esiste una pluralità di offerta, peraltro, con varietà di prezzi già molto ampia. Va da sé che la nostra strada non può essere che quella. Probabilmente all'inizio li abbiamo mantenuti allineati o non sicuramente uno superiore all'altro e poi, a mano a mano che si fa strada una funzionalità, evidentemente viene privilegiata.

PRESIDENTE. Ringrazio l'ingegner Sarmi, amministratore delegato di Poste italiane, per il suo intervento e per il documento depositato, di cui autorizzo la pubblicazione in allegato al resoconto stenografico della seduta odierna *(vedi allegato)*.

Dichiaro conclusa l'audizione.

La seduta termina alle 11,55.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE

DOTT. VALENTINO FRANCONI

Licenziato per la stampa
il 13 luglio 2012.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

Posteitaliane

Indagine conoscitiva sulla sicurezza informatica delle Reti

15 Maggio 2012

ALLEGATO

Agenda

Poste Italiane…

- La Missione
- L'infrastruttura tecnologica ed i sistemi di monitoraggio
- Le piattaforme di servizio

…e l'impegno nella Sicurezza

- I rischi ed i principali trend in atto
- L'impegno di Poste Italiane nella Cyber Security
  - La Fondazione Global Cyber Security Center
  - La European Electronic Crime Task Force
  - Il progetto .Post
- L'Identità Digitale

Posteitaliane

La missione di Poste Italiane

Diventare **un'azienda di servizi ad alto valore aggiunto che, valorizzando i suoi asset** fondamentali ed in particolare **la presenza capillare sul territorio, soddisfi le specifiche necessità della clientela tutta, nelle sue molteplici articolazioni,** con una **ampia ed integrata offerta di servizi** costruiti sulle proprie **competenze logistico/postali, finanziarie, di gestione dei processi di "outsourcing".**

Strumento fondamentale per il conseguimento di questi obiettivi è l'uso **di tecnologie Informatiche e di Telecomunicazione (ICT) all'avanguardia dirette alla costituzione del sistema "a rete" tra i più avanzati, completi e capillari del Paese.**

→ **Poste Italiane basa la propria missione sull'innovazione e sull'utilizzo di strumenti tecnologici all'avanguardia**

Posteitaliane

Agenda

Poste Italiane…

- La Missione
- **L'infrastruttura tecnologica ed i sistemi di monitoraggio**
- Le piattaforme di servizio

…e l'impegno nella Sicurezza

- I rischi ed i principali trend in atto
- L'impegno di Poste Italiane nella Cyber Security
  - La Fondazione Global Cyber Security Center
  - La European Electronic Crime Task Force
  - Il progetto .Post
- L'Identità Digitale

Posteitaliane

L'infrastruttura di Posteitaliane

RETE FISICA

- 14.000 Uffici postali
- 3.100 Uffici di recapito
- 22 centri meccanizzati

INFRASTRUTTURA ICT

- 11.000 uffici postali collegati in banda larga ad oltre 2Gbps
- Rete di trasmissione IP ad elevata capacità
- 5 Data Center che garantiscono anche il Disaster Recovery e la Business Continuity
- Datawarehouse con 37 mln di clienti
- Monitoraggio in tempo reale h24

RETE LOGISTICA

- 39.000 mezzi
- 4.500 corrieri
- 320 articolati
- 5 aerei (10 voli giornalieri)
- 3 hub logistici automatizzati

RETE DI ACCESSO MULTICANALE

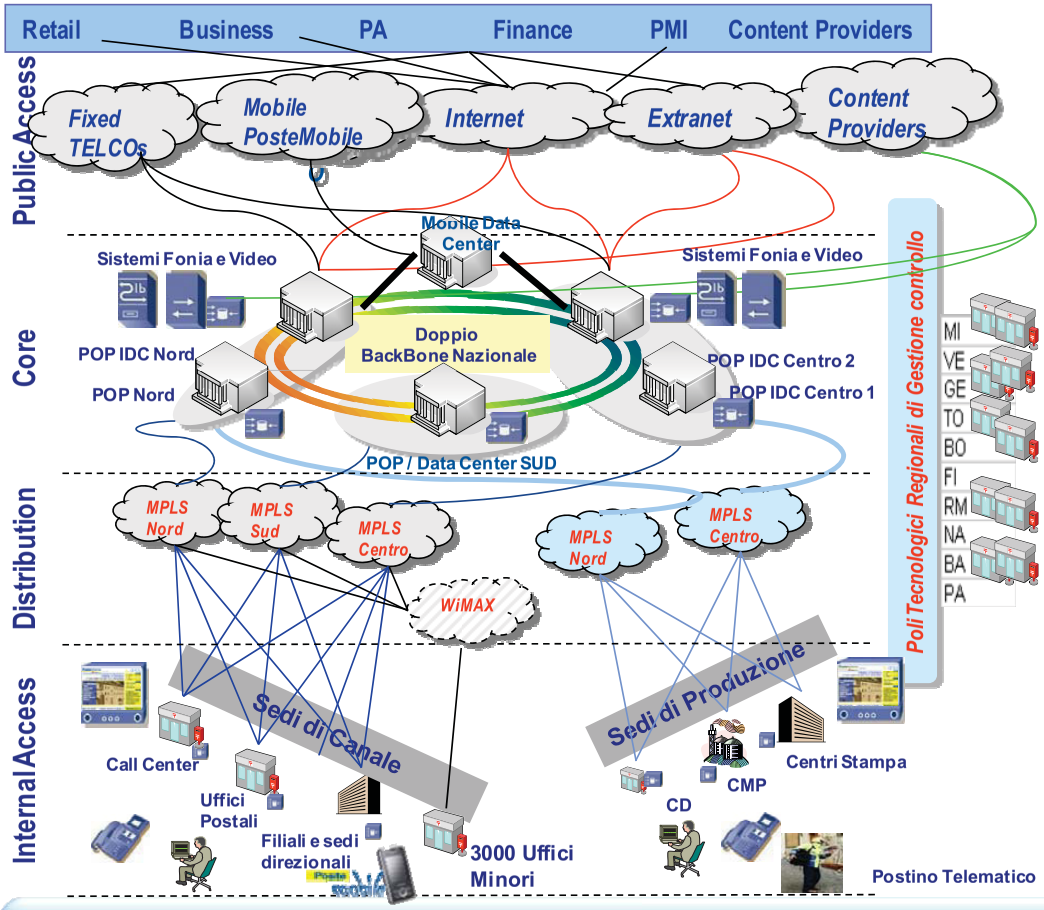
- 70.000 postazioni di lavoro
- Contact Center con 900 operatori
- Canale web con oltre 70 milioni di pagine visitate ogni mese
- 18.500 Portalettere dotati di terminale per l'erogazione di servizi mobili

- 6100 ATM (distributori di monete)
- 700 chioschi multimediali
- Telefonia cellulare

➔ Posteitaliane dispone di **una infrastruttura integrata**, che si compone di una **rete ICT** che offre supporto e connettività alla **rete fisica, alla rete logistica e alla rete di servizi mobili** di Poste e garantisce la possibilità di accedere in multicanalità a tutti i servizi

Posteitaliane

L'infrastruttura di rete TLC di Posteitaliane



Connettività Internet 800 Mps	612 extranet per *Partner Fornitori Clienti*
Connettività extranet 2520 Mps	

BackBone / Distribuzione
BackBone 2 Backbone Ottici Nazionali ridondati con banda fino a 10 Gbps
5 Reti MPLS Regionali in Disaster Recovery e Business Continuity a livello di raccolta

Infrastrutture LAN / WAN	
Porte switch	1.045.030
Router	30.750
Porte SAN	7.500
Firewall	150
Km fibra	125
Km rame	9.300
Post. di Lavoro	c,a, 70.000

Infrastrutture Fonia / Video	
Fonia / VoIP	> 66.000 terminali
	2 sistemi SoftSwitch ridondati ed in Business Continuity
IPTV	> 500 Sedi (previs. 1000)
	Regia Centrale
	Content Delivery Network
Sedi in Larga Banda	Sedi di Canale c.a. 14000
	Sedi Industriali c.a. 3500

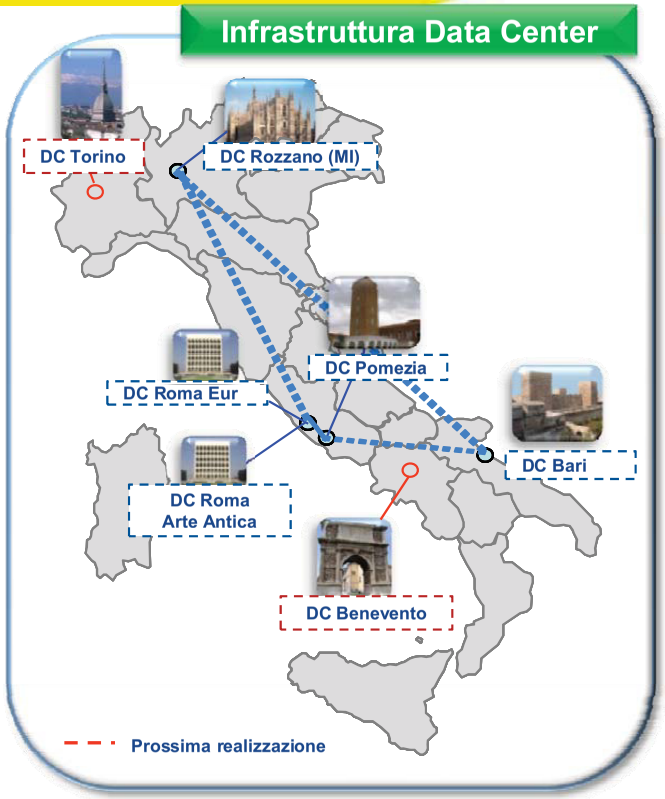
➔ **Un'infrastruttura di rete TLC a banda larga per il collegamento di tutti i siti (circa 20 mila) su protocollo IP, inclusi i più isolati, con un backbone ottico ad una velocità di 10 GBps che collega i 5 Data Center Nazionali integrando funzionalità di Business Continuity e Disaster Recovery**

Posteitaliane

I Data Center e il Piano di Business Continuity e Disaster Recovery

- **5 Data Center**
- Roma Arte Antica
- Roma Congressi
- Pomezia
- Bari
- Rozzano

- **2.240 Server Fisici** ed **oltre 1.700 Server Virtuali**
- Infrastruttura di Storage
  - **2,4 PetaByte** di spazio dati
  - **Infrastruttura di Cloud Storage** di **1 PetaByte** (espandibile fino a 14 PetaByte)



➔ **L'attuale Infrastruttura composta da 5 Data Center (a cui si aggiungeranno quelli di Torino e Benevento) , consente, oltre all'elaborazione, di effettuare il backup istantaneo di dati e applicazioni.**

➔ **Tale soluzione assicura, in un'ottica di Disaster Recovery, tempi di ripristino dell'operatività in brevissimo tempo, garantendo al contempo l'assoluta integrità dei dati.**

Posteitaliane

Le Sale di controllo: il monitoraggio e la gestione in tempo reale dell'infrastruttura

Service Control Area

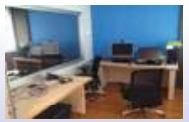

Service Control Room

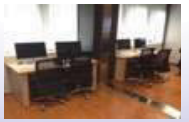

Logistic Control Room


Parcels Control Room


Security Room


Control Room Immobiliare


Internet Lab


Cybersecurity


Demo Room

European Electronic Crime Task Force

Electronic Crime Task Force

- Monitoraggio in tempo reale H24 dell'infrastruttura IT, dei processi logistici, dei servizi e della sicurezza delle transazioni
- Innovazione
- Sperimentazione dei nuovi servizi e contributo alla service creation grazie al supporto di community dedicate e al confronto con i clienti
- Sperimentazione su online e nuovi canali
- Contrasto del crimine informatico e costante ricerca di soluzioni per la protezione dei clienti

➔ Service Control Area garantisce il controllo, la sicurezza e l'innovazione dei servizi

Posteitaliane

Agenda

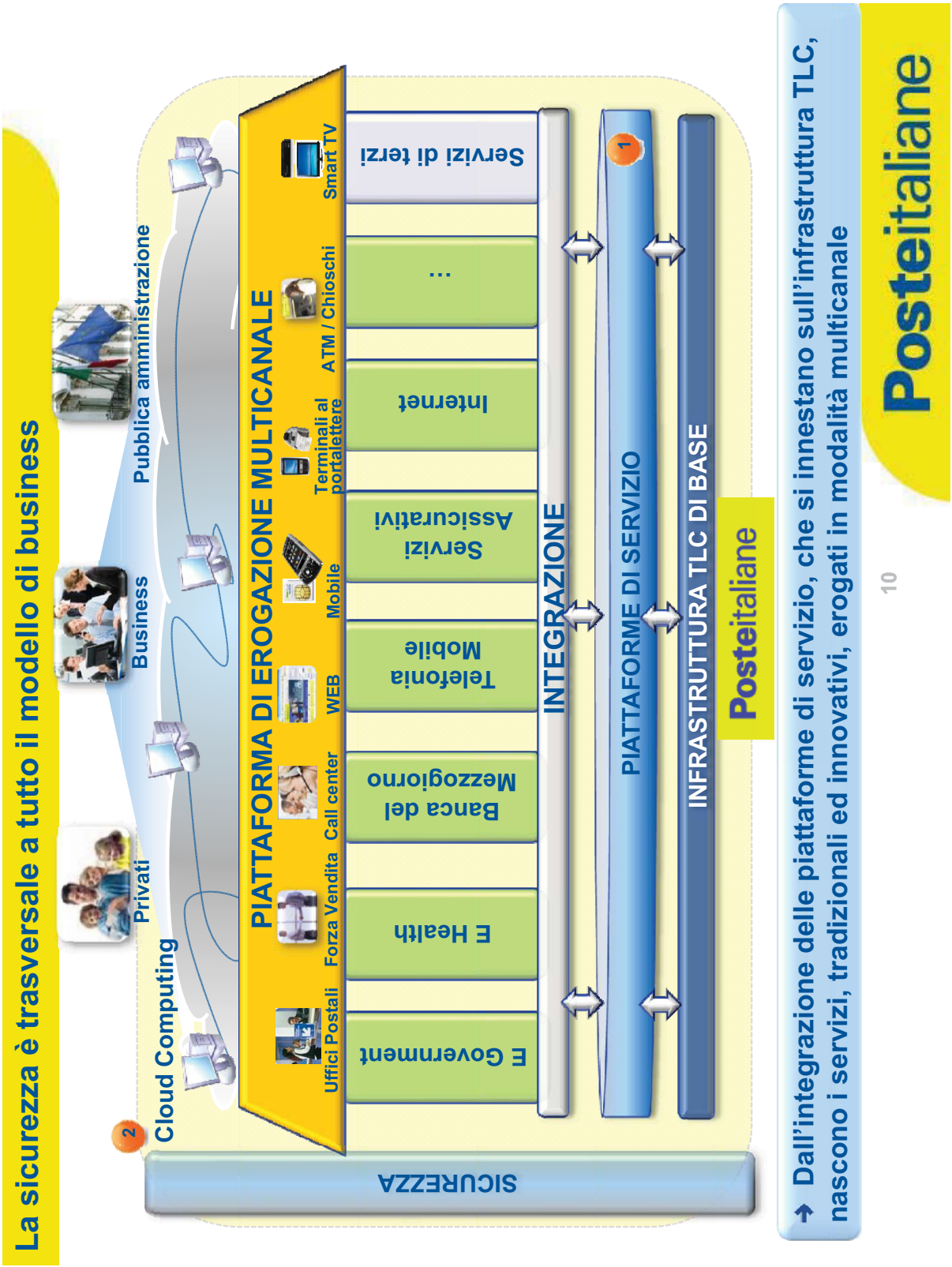
Poste Italiane…

- La Missione
- L'infrastruttura tecnologica ed i sistemi di monitoraggio
- **Le piattaforme di servizio**

…e l'impegno nella Sicurezza

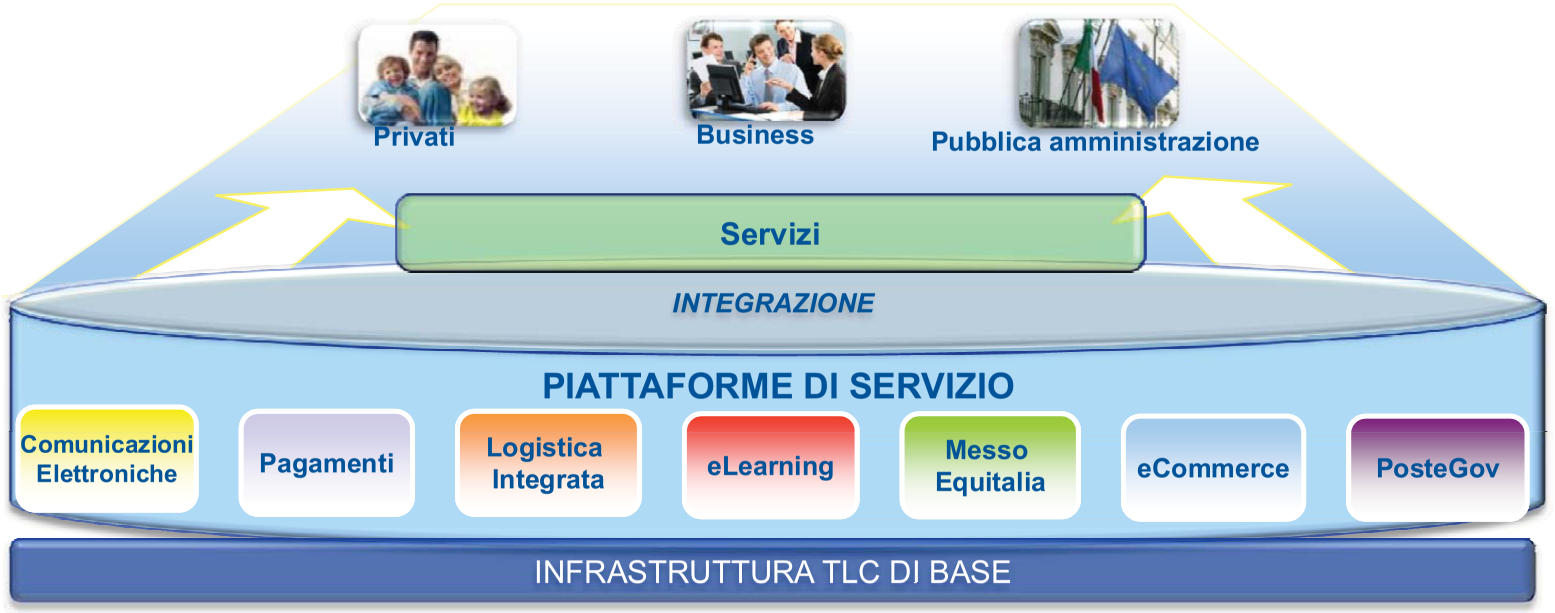
- I rischi ed i principali trend in atto
- L'impegno di Poste Italiane nella Cyber Security
  - La Fondazione Global Cyber Security Center
  - La European Electronic Crime Task Force
  - Il progetto .Post
- L'Identità Digitale

Posteitaliane


La sicurezza è trasversale a tutto il modello di business
Pubblica amministrazione
Business
Privati
Cloud Computing
2
PIATTAFORMA DI EROGAZIONE MULTICANALE
Uffici Postali
Forza Vendita
Call center
WEB
Mobile
Terminali al portalettere
ATM / Chioschi
Smart TV
E Government
E Health
Banca del Mezzogiorno
Telefonia Mobile
Servizi Assicurativi
Internet
...
Servizi di terzi
INTEGRAZIONE
1
PIATTAFORME DI SERVIZIO
INFRASTRUTTURA TLC DI BASE
Posteitaliane
SICUREZZA
Dall'integrazione delle piattaforme di servizio, che si innestano sull'infrastruttura TLC, nascono i servizi, tradizionali ed innovativi, erogati in modalità multicanale
Posteitaliane
10

Le piattaforme di servizio abilitate dall'infrastruttura ICT

1



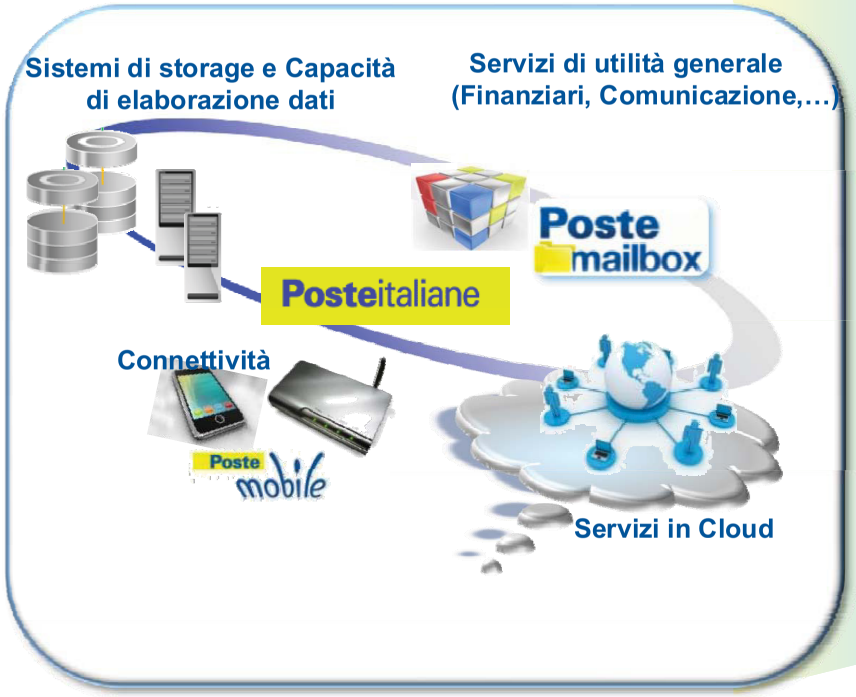
Le Piattaforme di servizio di Poste Italiane sono modulari, integrabili, possono essere rapidamente connesse con i sistemi e le reti di terzi e gestiscono in tempo reale oltre 50 milioni di transazioni al giorno

Posteitaliane

Il Cloud di Posteitaliane

2

L'infrastruttura di computing e storage, le piattaforme di servizio e di accesso multicanale



SaaS (Software as a Service) e PaaS (Platform as a Service)

Fiscalità e Servizi Sanitari	Gestione Documentale
E/M-Commerce	Piattaforma dei pagamenti
Comunicazioni Elettroniche	…….

Offerta digitale

IaaS (Infrastructure as a Service)

Architettura Applicativa e Sicurezza	Infrastruttura di rete
Infrastruttura Virtuale	Data Center
Sistemi di gestione	

Asset Fisici

➔ Posteitaliane, tramite la propria infrastruttura e l'accordo con importanti player internazionali, (SAP, Accenture,Selex Elsag…) può offrire alla PA, alle imprese e ai cittadini, servizi comuni e trasversali, in modalità sicura e ad alta affidabilità con tempi brevi di realizzazione

Posteitaliane

Agenda

Poste Italiane…

- La Missione
- L'infrastruttura tecnologica ed i sistemi di monitoraggio
- Le piattaforme di servizio

…e l'impegno nella Sicurezza

- **I rischi ed i principali trend in atto**
- L'impegno di Poste Italiane nella Cyber Security
  - La Fondazione Global Cyber Security Center
  - La European Electronic Crime Task Force
  - Il progetto .Post
- L'Identità Digitale

Posteitaliane

Evoluzione del panorama del cyber crime

Internet:
Rete globale complessa e vulnerabile

Vettori di attacco multipli

Varietà di strumenti tecnologici e di social network

OBIETTIVI E BERSAGLI

UTILIZZATORI SINGOLI
- Furto di identità
- Home banking/ carte
- Inclusione in Botnet

PICCOLE AZIENDE
- Conti bancari online
- Danneggiamento del business/ concorrenza

GRANDI AZIENDE
- Attacchi mirati
- Data Breaches
- Distributed Denial of Services attack

GOVERNI
- Cyber Spionaggio
- Hacktivism
- Cyber Sabotaggio

Posteitaliane

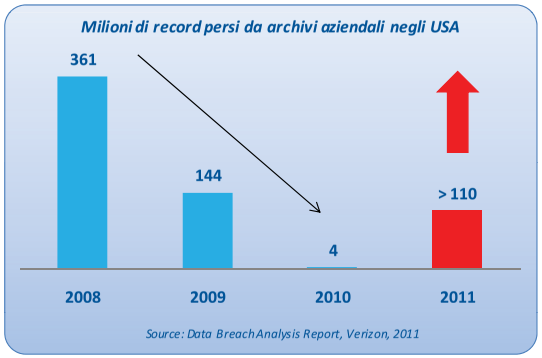
La fenomenologia degli attacchi

BOTNET

- rilevate 240.000 infezioni giornaliere originate delle 7 botnet principali
- Italia 3° paese più attaccato al mondo da botnet ZeuS
- Oltre 6.000.000 pagine web sono compromesse da malware per drive-by-download

Attacchi ad ARCHIVI AZIENDALI

- Le informazioni contenute negli archivi aziendali sono l'obiettivo delle nuove forme di attacco.
- Il 2011 fa segnare un'inversione di tendenza rispetto al precedente triennio



Attacchi ad utenti: FURTO DI IDENTITA

- Le azioni di protezione delle proprie informazioni sull'identità si concretizzano per l'utente in pratiche di sicurezza che si limitano nella maggior parte dei casi all'ambito delle sole frodi su carta, mentre molta meno attenzione sembra venir posta all'ambito dell'operatività su Internet.

Ultimi casi

- **2012:** hacker rubano a Global Payment dati di 1,5 milioni di carte di credito Visa e MasterCard in Nord America
- **2011:** furto di 77 mln di dati di carte di credito a Sony con danni stimati per 172 mln $

Negli ultimi anni si sta assistendo ad un aumento degli attacchi sia verso il singolo utente sia verso Aziende ed Istituzioni, in particolare indirizzati ad infrastrutture e servizi di carattere strategico

Posteitaliane

Agenda

Poste Italiane…

- La Missione
- L'infrastruttura tecnologica ed i sistemi di monitoraggio
- Le piattaforme di servizio

…e l'impegno nella Sicurezza

- I rischi ed i principali trend in atto
- **L'impegno di Poste Italiane nella Cyber Security**
  - La Fondazione Global Cyber Security Center
  - La European Electronic Crime Task Force
  - Il progetto .Post
- L'Identità Digitale

Posteitaliane

L'impegno di PosteItaliane nella Cyber Security

Monitoraggio e gestione H24 / 7 giorni su 7

Infrastruttura dei Data Center E il piano di Business Continuity e Disaster Recovery

Presidio della sicurezza :

- delle infrastrutture
- della rete
- dei dati
- delle informazioni

Ricerca e sviluppo

➔ **Poste Italiane pone tra le proprie priorità la sicurezza delle infrastrutture, dei canali di accesso e delle comunicazioni elettroniche.**

Posteitaliane

La Fondazione Global Cyber Security Center

- **Poste Italiane** ha costituito nel 2010 una fondazione con scopo primario la cyber security
- **Obiettivi della Fondazione sono:**
  - **diventare un polo di aggregazione della conoscenza sul cyber crime**
  - **supportare le organizzazioni italiane ed internazionali nell'acquisire conoscenza ed esperienza sul tema;**
  - **contribuire allo sviluppo di nuove soluzioni** organizzative, procedurali e di regolamentazione **per meglio proteggere cittadini, governi e organizzazioni private**
- Tali obiettivi vengono perseguiti attraverso un impegno costante nella **ricerca, formazione e promozione dello scambio delle informazioni** fra pubblico e privato sia a livello nazionale che internazionale.

- **I partner:**

La European Electronic Crime Task Force

European Electronic Crime Task Force

➔ La **Fondazione Global Cyber Security Center (GCSEC) e Poste Italiane** fanno parte **della European Electronic Crime Task Force** creata con US Secret Service e Ministero degli Interni nel 2009 e con obiettivo la creazione di una alleanza strategica tra forze dell'ordine, università e settore privato finalizzata all'identificazione e mitigazione di attività di Electronic Crime (eCrime)

European Electronic Crime Task Force

Posteitaliane

polizia delle comunicazioni

La Mission

"Sostenere l'analisi e lo sviluppo delle "Best Practices" contro la cybercriminalità nei paesi europei attraverso la creazione di un'alleanza strategica tra forze dell'ordine, il mondo accademico, giuridico ed enti del settore privato

Le attività

Organizzazione di **Meeting trimestrali** per la **condivisione di informazioni** con gli addetti del settore per la costruzione di nuove **alleanze strategiche** e lo sviluppo di una comprensione comune delle minacce e tecniche per il contrasto.

Realizzazione di **Concept** e **simulazioni di scenari di attacco**, relativi alle tematiche del cybercrime,

Monitoraggio costante delle **novità in materia di cybercrime**

Redazione di **Newsletter bimestrali e Report annuali** sui trend relativi alle nuove minacce informatiche

Posteitaliane

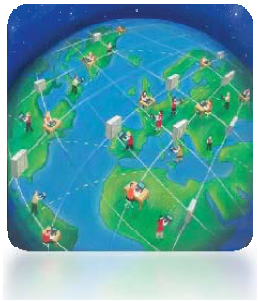
Il Progetto ".post"

.post

ICANN

- Con l'importante contributo di Poste Italiane, nel 2009 l'Unione Postale Universale (UPU), ha ottenuto da ICANN il dominio sponsorizzato di primo livello **".post"** dedicato agli operatori postali, ai loro partner e clienti:
- un ambiente unico e riservato al settore postale nel mondo.
- grazie ad un set di regole (es.: utilizzo DNSSec) di cui Poste Italiane è stato il principale estensore, garantirà il **massimo livello di sicurezza possibile**, condizione indispensabile per la nascita dei nuovi servizi internazionali di comunicazione elettronica sicura

- Il dominio ".post" consentirà di:
- trasferire nel mondo digitale l'affidabilità ed il ruolo di Terza Parte Garante da sempre riconosciuti agli operatori postali, rafforzandone ulteriormente il brand
- armonizzare i livelli di sicurezza e certificazione delle comunicazioni e delle transazioni internazionali
- consentire l'identificazione in maniera certa (identificazione forte) di tutti gli attori della catena del valore nelle transazioni digitali sul dominio (es.: service providers, clienti, ecc.)
- sviluppare servizi digitali realmente interoperabili



Nuovi servizi al cittadino in ambito internazionale

- Comunicazioni digitali certificate (es.: PReM – Postal Registered electronic Mail)
- e-Government (es.: erogazione certificati per cittadini residenti all'estero)

Posteitaliane

Sinergie che consentono un'efficace azione di contrasto e prevenzione

L'azione di prevenzione e protezione di Poste Italiane si esplicita lungo la catena operativa Monitoraggio → Analisi → Contrasto,

MONITORAGGIO

- Prev Frodi circuito finanziario
- Prev Frodi Conti Online
- Comportamenti sospetti

ANALISI

- Analisi visuale scenari frode
- Apertura Prodotti Finanziari
- Analisi trasversale prodotti

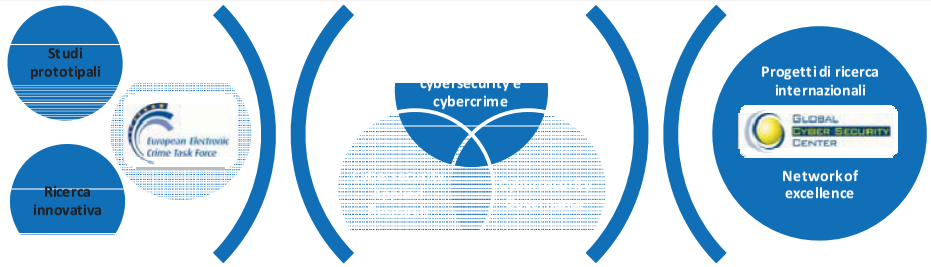
CONTRASTO

- Blocco ID compromessi
- Controllo Identità
- Blocco Carte e Conti
- BlackList frodatori

nel **2011** sono state verificate

15.483.533 identità

INNOVAZIONE, RICERCA E INTERNAZIONALIZZAZIONE



Cyber Security Competence Center

La sinergia tra le competenze interne, la European Electronic Crime Task Force e la Fondazione GCSEC è intesa a rafforzare la leadership del Gruppo Poste Italiane nella cybersecurity e porre l'azienda come attore di riferimento nel settore, con benefici diretti ed indiretti sul business, sul brand e nei confronti della clientela.

Posteitaliane

Agenda

Poste Italiane…

- La Missione
- L'infrastruttura tecnologica ed i sistemi di monitoraggio
- Le piattaforme di servizio

…e l'impegno nella Sicurezza

- I rischi ed i principali trend in atto
- L'impegno di Poste Italiane nella Cyber Security
  - La Fondazione Global Cyber Security Center
  - La European Electronic Crime Task Force
  - Il progetto .Post
- **L'Identità Digitale**

Posteitaliane

Identità digitale: il contesto normativo

➔ L'identità digitale in internet non è normata, esistono solo alcuni standard tecnici (ISO) e linee guida generali.

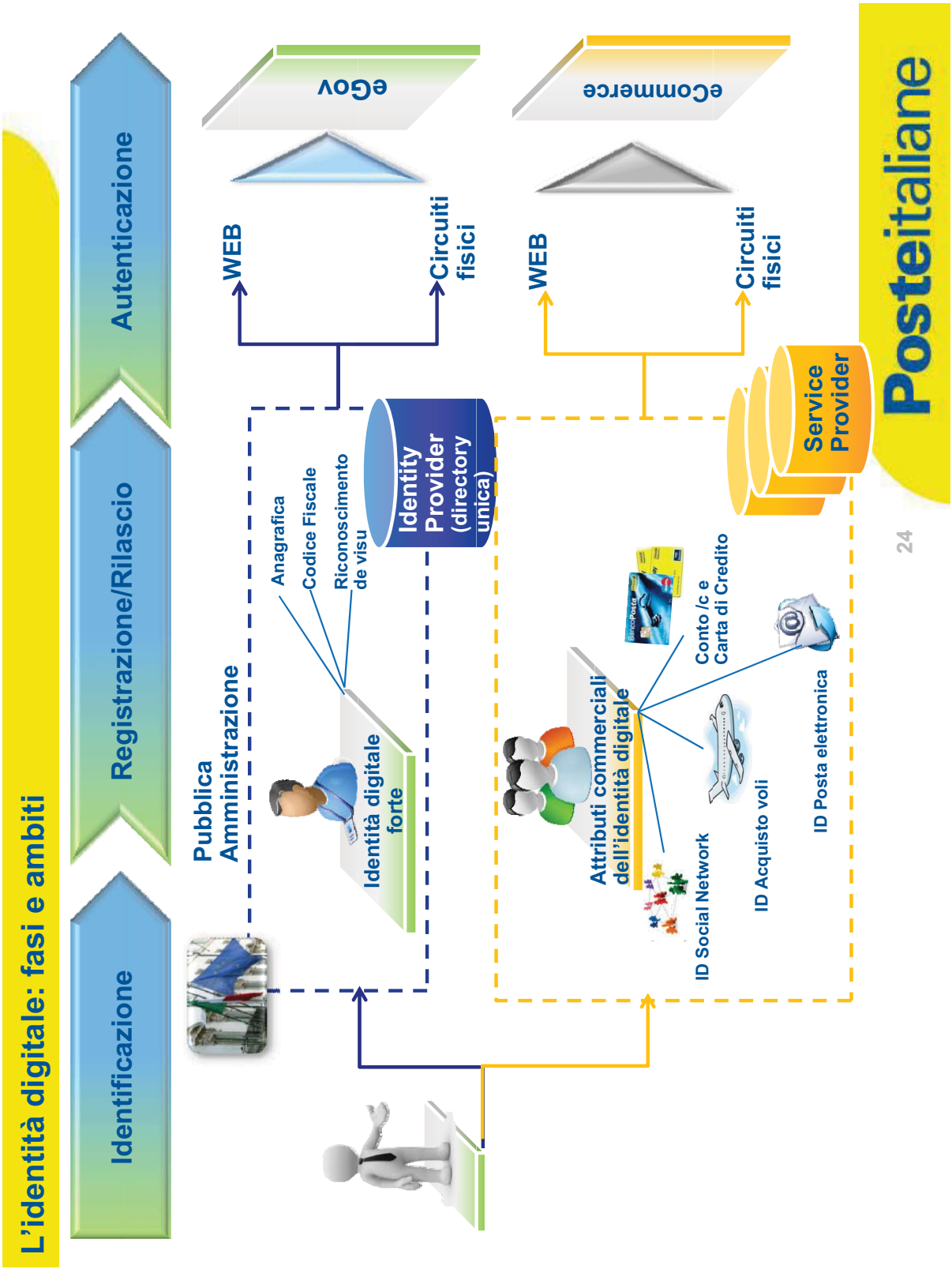
Internazionale

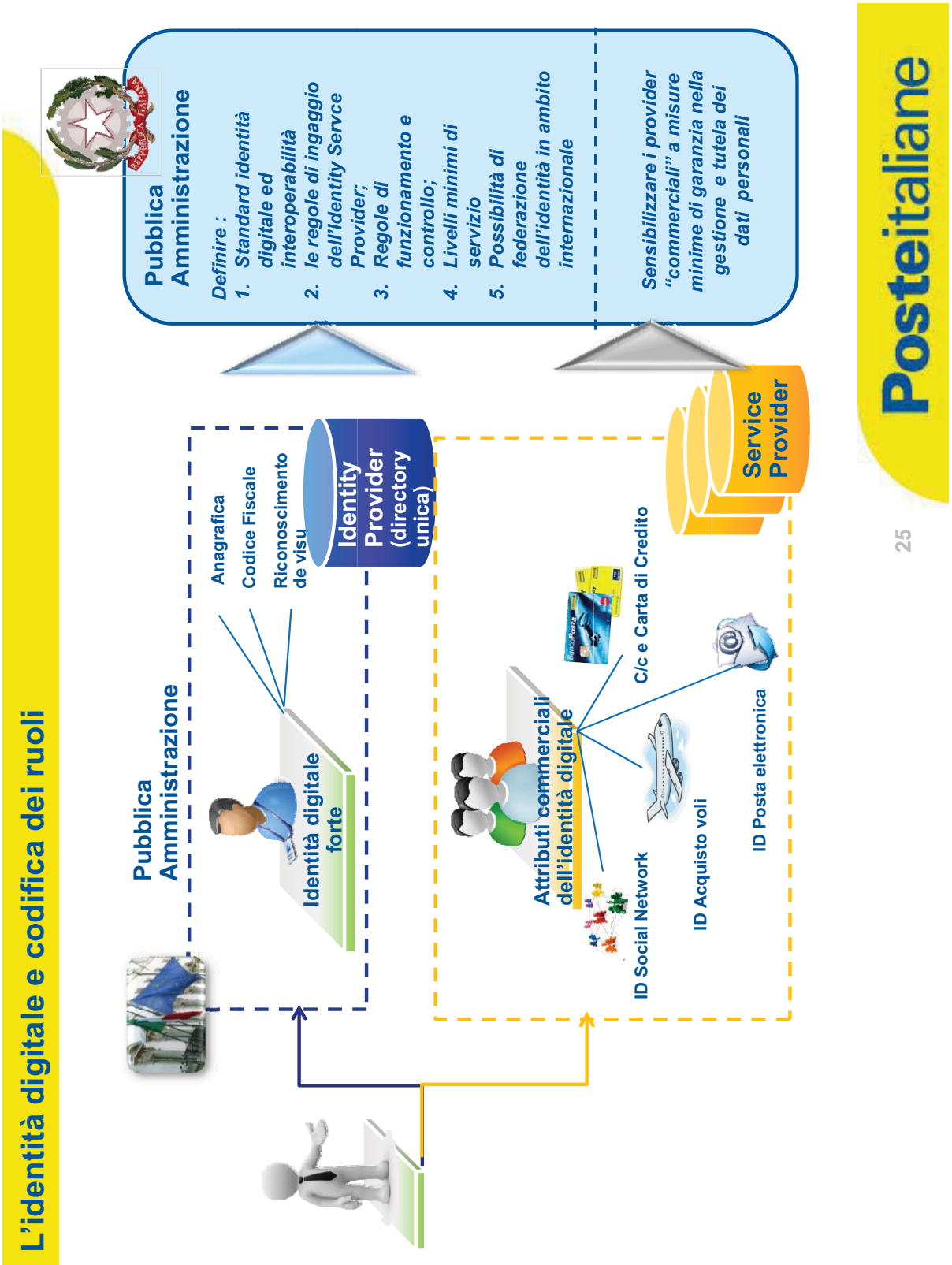
- Non esistono norme internazionali di ampio spettro che affrontano il tema dell'identità digitale.
- La normazione in materia si basa su standard tecnici che affrontano singoli aspetti come autenticazione, data management, privacy (es. Standards ISO), su principi e linee guida (NIST, OECD) e su standard de facto (OpenID, Persona, OneID)

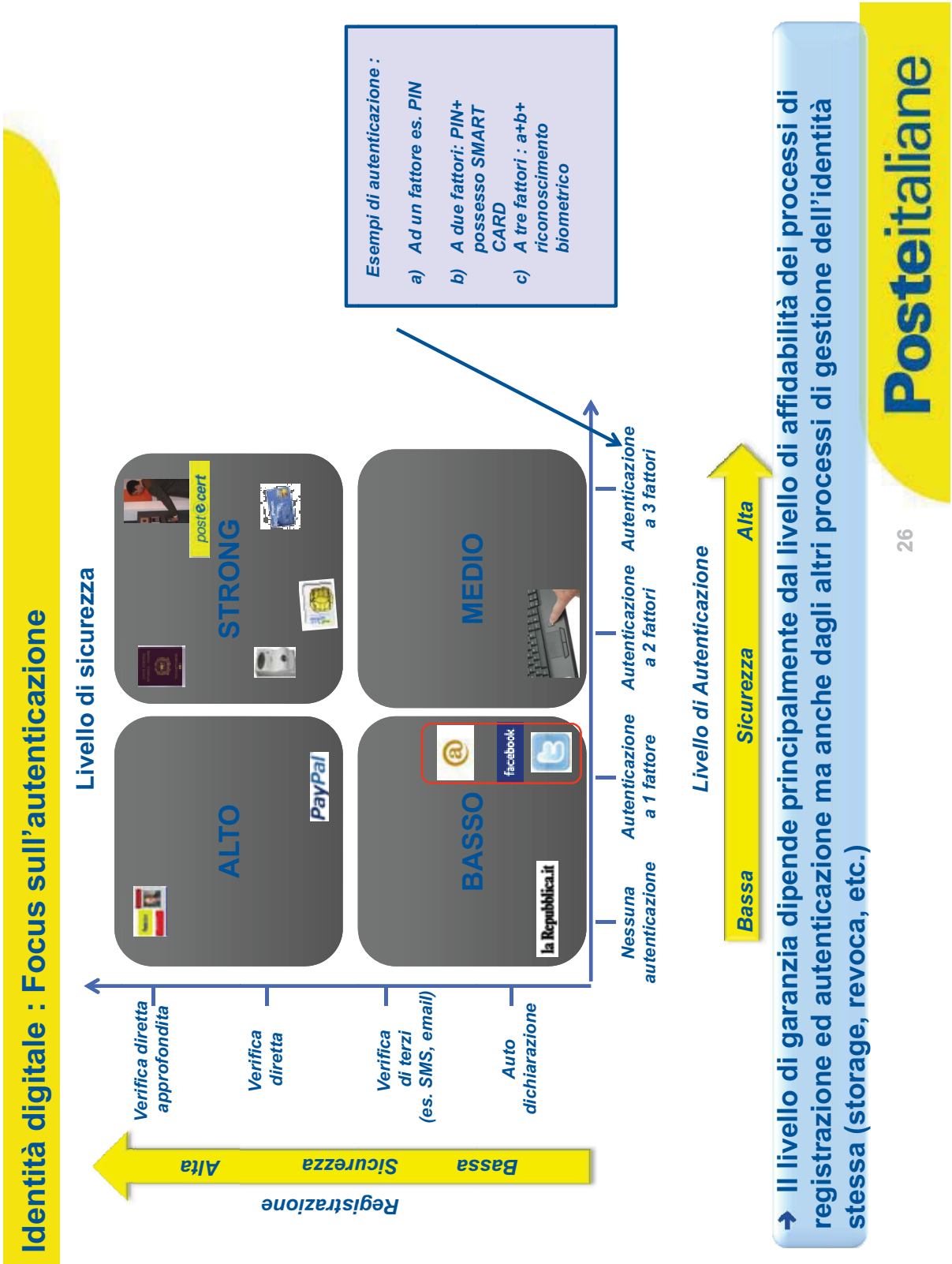
Nazionale

- Non esistono norme nazionali che regolino l'identità digitale
- Le uniche norme che marginalmente toccano tale tema sono relative a privacy e protezione dei diritti dell'individuo

Posteitaliane


L'identità digitale: fasi e ambiti
Identificazione
Registrazione/Rilascio
Autenticazione
Pubblica Amministrazione
Anagrafica
Codice Fiscale
Riconoscimento de visu
Identità digitale forte
Identity Provider (directory unica)
eGov
WEB
Circuiti fisici
eCommerce
WEB
Circuiti fisici
Service Provider
Posteitaliane
Attributi commerciali dell'identità digitale
Conto /c e Carta di Credito
ID Social Network
ID Acquisto voli
ID Posta elettronica
24


L'identità digitale e codifica dei ruoli
Posteitaliane
25
Pubblica Amministrazione
Definire :
1. Standard identità digitale ed interoperabilità
2. le regole di ingaggio dell'Identity Servce Provider;
3. Regole di funzionamento e controllo;
4. Livelli minimi di servizio
5. Possibilità di federazione dell'identità in ambito internazionale
Sensibilizzare i provider "commerciali" a misure minime di garanzia nella gestione e tutela dei dati personali
Service Provider
Identity Provider (directory unica)
Anagrafica
Codice Fiscale
Riconoscimento de visu
Pubblica Amministrazione
Identità digitale forte
Attributi commerciali dell'identità digitale
C/c e Carta di Credito
ID Posta elettronica
ID Acquisto voli
ID Social Network



€ 4,00

16STC0019340