PRESIDENZA DEL VICEPRESIDENTE SILVIA VELO

La seduta comincia alle 14,05.

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 e la trasmissione televisiva sul canale satellitare della Camera dei deputati.

Audizione del dottor Mario Magini, esperto di sicurezza informatica.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza informatica delle reti, l'audizione del dottor Mario Magini, esperto di sicurezza informatica.

Do la parola al dottor Magini per lo svolgimento della relazione.

MARIO MAGINI, *Esperto di sicurezza informatica*. Nell'ambito del programma dell'indagine conoscitiva, che riporta tutti i punti critici nella gestione della sicurezza in rete, vorrei portare un modesto contributo su un argomento che è un po' la madre di tutte le insicurezze e di tutti i problemi che possono presentarsi sulla rete.

Spendo innanzitutto alcune parole sullo scenario. I numeri di crescita dei servizi in rete sono a due cifre, ma in un ambiente estremamente variegato. Sicuramente sono a due cifre sui sistemi finanziari, sui sistemi di *e-commerce*, nonché sui sistemi di relazione fra i cittadini e la pubblica amministrazione, specialmente in sede di presentazione di istanze che portano con sé anche un valore economico.

Per esempio, nel settore dell'edilizia i professionisti parlano ormai con i comuni ed espongono istanze in maniera totalmente telematica. Non solo i pagamenti di diritti e oneri spesso vengono effettuati anch'essi in maniera telematica, ma addirittura anche l'autenticazione dell'avente titolo che presenta una pratica edilizia a un comune o del suo tecnico che deve avvenire con criteri rigorosi. Si tratta, infatti, anche di dati sensibili ed economici che riguardano il cittadino nella sua relazione con l'amministrazione.

È chiaro che la diffusione di servizi in rete, se ben costruiti, è utile. Tuttavia, non si diffonde in rete un servizio semplicemente facendo scaricare un modulo che poi va riempito a mano, inviato per fax e ridigitato dall'organico dell'ente ricevente. Questa non è una reale diffusione di servizi in rete, ma una bacheca pubblica di moduli.

La diffusione di servizi in rete, se efficiente, deve prevedere tutta l'interazione e, quindi, tutto il processo deve essere svolto in maniera telematica, con il grosso vantaggio che il *back office* dell'amministrazione titolare del procedimento registra in automatico i dati digitati dall'utente e convalidati con un'autenticazione adeguata alla materia.

Ogni autenticazione e ogni sicurezza coprono un livello di rischio percepito ed effettivo. Se i dati vengono trattati in maniera automatica, si risolve un problema molto grosso di tempi di smaltimento delle pratiche, con accorciamento di tutta la filiera del servizio, in quanto i

dati vanno a confluire nei sistemi informativi dell'ente che deve gestire il procedimento in maniera automatica.

Ponendoci in queste condizioni, e molte amministrazioni lo stanno già facendo, anche con livelli di eccellenza in taluni casi che abbiamo constatato, la filiera si accorcia. La tempestività è totale, perché parliamo di tempo reale e il livello di soddisfazione dell'utente è elevato, perché si trova di fronte a pochi errori. La ridigitazione comporta effettivamente errori, mentre, se si tratta di un documento che viene assunto *as is* dal *back office* dell'amministrazione, la probabilità di errori decade in maniera esponenziale.

L'abbattimento dei costi del servizio, come abbiamo anticipato, è un fattore sottostante, perché, evitando rilavorazioni di documenti, sicuramente tutto il costo del servizio si abbatte e si può anche immaginare un impiego molto migliore e comunque ottimale delle risorse dedicate attualmente a trattare i documenti in maniera semiautomatica.

I problemi principali, che sono in realtà due aspetti dello stesso problema, sono riservatezza e sicurezza. Chi approccia uno strumento informatico deve avere la garanzia di poter parlare con il *server* giusto.

Uno dei problemi di sicurezza più grossi che occorrono in questo momento e con cui si perpetra, peraltro, la maggior parte dei crimini informatici è il fatto che l'utente si trova davanti un *server*, ossia l'espressione tecnologica di un servizio, che per lui è quello a cui vuole indirizzare la sua domanda di servizio e il suo colloquio interattivo, mentre, invece, si tratta di un *server* finto utilizzato per carpire informazioni all'utente.

Tale evento invade immediatamente il campo del settore riservatezza, ma anche quello della sicurezza, perché il suddetto *server* può, a sua volta, presentarsi come un attacco di tipo *man in the middle*, cioè l'uomo nel mezzo. In questo caso in mezzo c'è il *server*, che colloquia con l'utente fingendo di essere il *server* vero e poi con il *server* vero, fingendo di essere l'utente.

Si tratta di un attacco che avevamo preconizzato già diversi anni fa, ma che per questioni anche tecnologiche, essendo un attacco non banale, non veniva spesso perpetrato. Io e altri colleghi che si occupano di sicurezza anche nel mondo interbancario – la mia provenienza è proprio dal mondo interbancario – avevamo preconizzato questo tipo di attacco, che nelle ultime decine di giorni è esploso in maniera anche molto preoccupante nei confronti di grosse entità finanziarie, come BancoPosta e alcune banche. Cito BancoPosta perché è emerso sulla stampa, ma siamo a conoscenza anche di attacchi perpetrati con lo stesso identico sistema nei confronti di istituzioni finanziarie.

Sono attacchi molto pericolosi perché, al di là dell'effetto economico che possono generare, creano immediatamente una percezione di insicurezza e di sfiducia che mina alla base la possibilità di promuovere il progresso facendo accettare come sicure e riservate le transazioni che vengono effettuate in rete.

Come è noto, gli utenti usufruiscono di servizi telematici a distanza per comodità. Un servizio telematico è anche il *phone banking*. Porto l'esempio della mia vecchia zia, che telefona alla banca, alla quale la banca chiede la *password* per poter entrare. Opera a livello telefonico perché magari è meno avvezza a uno strumento più tecnico o tecnologico, però è una persona sveglia, anche se ha novant'anni, e conosce il livello di sicurezza. Compie, comunque, in effetti un'operazione telematica a distanza: adopera il telefono dall'altra parte del quale c'è un operatore, ma nella sostanza dell'operazione non cambia nulla rispetto a un'operazione tramite PC o magari, per i più sofisticati, tramite un *app* sull'iPhone o su un altro strumento mobile, come gli smart-phone con sistema operativo Android.

L'utente vuole usufruire di servizi di *provider* diversi – come *service provider* si possono intendere una banca, una pubblica amministrazione o qualunque altro soggetto – su *media* diversi e con strumenti tecnologici diversi. Il concetto del-

l'ubiquità – *anywhere, anytime*, dove sono e in qualunque momento – è la base perché la telematizzazione, che potrebbe comportare miliardi e miliardi di euro di risparmi sia per la pubblica amministrazione, sia per le entità private che offrono servizi in rete, venga minata fortemente dall'impossibilità di operare con gli stessi mezzi dappertutto e con le stesse modalità d'uso.

Qual è il problema dello stato attuale ? Io penso che sia una questione che riguarda tutti noi. In questa sala tutti noi siamo sicuramente in possesso di credenziali per accedere ad alcuni siti, però ci sono credenziali per la Ryanair, per l'Alitalia, per l'INPS, per il comune di Roma, se si vive a Roma, per il comune di Reggio Emilia, se si vive a Reggio Emilia.

Siamo dotati di una serie sempre più crescente di *password*, ciascuna delle quali è dedicata a un singolo servizio. Ora tiro fuori un oggetto che vorrei mostrare, perché sicuramente l'abbiamo tutti, ossia la cartucciera dei dispositivi di autenticazione. La mia comprende il dispositivo per la BNL, quello per l'UniCredit e quello per il Monte dei Paschi di Siena. Per tre banche ci sono tre dispositivi e tre modi diversi di accedere.

Parliamo di *one-time password*, cioè di *password* da bruciare, i dispositivi più sicuri sul mercato per l'autenticazione. Che cosa comportano ? Gli utenti dispongono di una rastrelliera di credenziali e succede un fatto brutto, anzi bruttissimo. Essi memorizzano queste credenziali, quando non si tratta di oggetti fisici come quelli che vi mostro, ma più leggeri, come la *password* delle Mille Miglia, su pezzettini di carta. Nella mia carriera, anche in ambienti sicuri come le banche, ho visto *password* memorizzate con Post-it sullo schermo. Parliamo di *password* dispositive che nell'*overnight* possono muovere un miliardo di euro, non un milione di euro. Stiamo parlando di imprudenze organizzative dovute, però, alla tremenda complicazione di dover gestire molte coppie di credenziali. Le credenziali si perdono perché si dimenticano. Se, invece, si è molto astuti, si mettono in un mezzo che si può controllare, cioè il telefonino.

Apro una parentesi che vi farà sorridere. Un maresciallo dei Carabinieri di una stazione di campagna aveva catturato alcuni signori di nazionalità imprecisata, che avevano escogitato una truffa, divenuta poi nota, ai bancomat: collocavano un'interfaccia sopra la tastiera del bancomat e intercettavano i codici mentre si passavano le carte, un trucco molto sofisticato. Avevano poi inserito in un PC tutti i numeri di bancomat e i PIN e si stavano accingendo a svuotare i conti dei clienti. È una minaccia pericolosa, perché questi soggetti prelevano 200-300 euro per volta e prima che il cliente si accorga dell'avvenuto reato, loro hanno comunque fatto man bassa.

Questo maresciallo, che è molto bravo in informatica, con un suo computer stava cercando di individuare la chiave di questo *repository*, ossia di questo *database*, in cui evidentemente, considerata la dimensione, erano sicuramente conservati numeri bancomat e PIN. Essi erano stati cifrati, però, con una *password* e con un metodo di cifratura molto forte, a livello quasi militare.

Alla fine il maresciallo ipotizzò che avrebbe impiegato alcuni giorni. Io gli risposi che mi dispiaceva di deluderlo, ma che ci avrebbe impiegato alcuni milioni di anni, perché gli strumenti attuali computazionali per poter, come si dice in gergo, « crackare a forza bruta » una *password* di sicurezza possono impiegarci molti e molti anni, anche nel caso degli strumenti più potenti. Domandai, però, se avessero sequestrato i telefonini. A quel punto, lui comprese. Chiaramente la *password* era nel telefonino. Ciò significa che anche il ladro più accorto alla fine memorizza le *password* nel telefonino e io scommetto che anche qualcuno di noi lo fa.

È un problema, perché poi ciò che è stato inserito nel telefonino con un finto prefisso, trucchi che tutti utilizziamo, ma che sono un po' infantili, espone a un attacco con la sottrazione del telefonino, il

che diventa devastante, perché così i ladri possiedono tutte le *password*, quella della Banca, quella dell'Alitalia e via elencando.

Ci sono altri che adottano una strategia in apparenza più intelligente. Per tutti i servizi cercano di adottare la stessa *password*, in modo da ricordarla e non doverla scrivere. Questo è il massimo della disgrazia, perché ci sono alcuni servizi, come quelli finanziari, che sono molto protetti, ragion per cui è difficilissimo per un *intruder*, per un *hacker* e anche per un *insider* – i danni vengono compiuti spesso dall'interno dell'organizzazione e non sempre da fuori – entrare. La storia degli *hacker* è tutta da discutere, ma non è questo il momento di farlo.

È chiaro, però, che, se si accede, invece, a un sito di viaggi o di *e-commerce* un po' leggero e si è adottata la stessa *password*, chi vuol colpire, colpisce nell'anello debole della catena, non in quello forte, ragion per cui cattura la *password* nel punto meno presidiato dal punto di vista della sicurezza e poi l'adopera per agire sul conto corrente.

Il comportamento normale dell'utente comporta un livello di sicurezza veramente basso, con rischio di furto di identità, perché, quando sono state sottratte le credenziali, chi le ha sottratte si presenta come il titolare e lo è a tutti gli effetti, dal momento che non c'è alcun sistema per cui l'interlocutore telematico (fornitore di servizio) possa stabilire se lo è o non lo è, a meno di utilizzare sofisticati metodi di autenticazione, cui accenneremo molto rapidamente.

Soprattutto l'utente non solo deve memorizzare coppie di *username* e *password*, ma deve anche avere dimestichezza con strumenti digitali diversi. Nella mia borsina, se li ritrovo, ci sono strumenti che adopero tutti i giorni e che mi porto dietro, come la *smart card* di firma elettronica rilasciata da una *Certification Authority* nazionale, uno strumento ipersicuro, che equivale come sicurezza alla CIE e per l'autenticazione anche alla CNS, ossia alle carte ufficiali sia dello Stato, sia regionali.

Esiste un lettore di *smart card*, ma devo aver installato nel mio PC un *software* apposito. Se lo metto in un altro PC, non mi autentico, non succede nulla. Devo, dunque, disporre di una batteria di oggetti con modalità d'uso differenti e questa è un'altra barriera fortissima alla diffusione dei servizi telematici.

Andiamo a vedere, invece, che cosa succede, sempre rapidamente, dal lato dei *service provider*, ossia dei fornitori di servizi, quali pubblica amministrazione, locale e centrale, sistemi finanziari, sistemi di *e-commerce* o sistemi di viaggio, come Trenitalia.

Al giorno d'oggi, tranne rarissimi casi di interoperabilità – l'unico rilevante è forse quello dell'Agenzia delle entrate – ogni *service provider* ha un suo sistema di assegnazione delle credenziali digitali. Alcuni sono forti, sono *de visu*, ragion per cui ci si deve recare a uno sportello, ma quel fornitore di servizi deve avere uno sportello, altrimenti sono dolori o comunque si deve convenzionare con uno sportello improbabile che assegni l'identità *de visu*, cioè guardi l'utente negli occhi, controlli il documento e attribuisca l'identità digitale. È un sistema che deve coesistere nei suoi sistemi informativi e che costa molto impostare, a livello sia gestionale, sia operativo. Meno sportelli sul territorio il gestore ha e più è complicato, perché deve stipulare convenzioni con terzi.

Il secondo lato dell'identità digitale è la gestione del sistema di autenticazione, che è una vera applicazione informatica. Poniamo che io eroghi cinque servizi al cittadino, come il SUAP, le mense scolastiche, il pagamento delle multe *online*. Utilizzo diversi sistemi e davanti a tutti questi sistemi di servizio, quando sono ben impostati, c'è un sistema di autenticazione. Ci sono anche esempi deprimenti di grandi entità che hanno un sistema di autenticazione per ogni applicazione, se Dio vuole, almeno stanno tranquilli, ma generano una grande complicazione all'utente.

La funzione di garantire l'identità digitale di una persona, di un cittadino o di un'entità che si presenta a una seconda

entità richiede un'infrastruttura, naturalmente informatica, di autenticazione e di gestione degli accessi. Un *service provider*, quindi, deve mettere in campo solo per la questione di riconoscere il suo interlocutore tutti gli oggetti che abbiamo elencato. Non ve li sto a elencare tutti, ma sicuramente deve impiantare un sistema di assegnazione e di distribuzione delle credenziali, produrre oggetti *card* o altri ammennicoli come quelli che abbiamo mostrato poco fa e gestirne il ciclo di vita.

Le *password*, infatti, non possono essere statiche per tutta la vita, altrimenti si rendono possibili i cosiddetti attacchi « a dizionario ». Poiché la nostra fantasia nel generare *password* è molto limitata, ci sono leggende metropolitane in merito molto concrete. Si parte dal nome della moglie, se si ha un amante dal nome e dalla data di nascita dell'amante, per arrivare al nome del figlio o del cane, o anche a un numero improbabile, come una data, che però bisogna ricordare e viene, dunque, associato a un evento della propria vita.

Ciò significa che negli attacchi cosiddetti « a dizionario », in cui sono elencate le *password* più frequenti nell'uso comune di tutti noi, se la *password* dura un periodo limitato di tempo, prima o poi viene rubata e con essa anche l'identità.

Gestire il ciclo di vita anche di una sola *password* comporta obbligare l'utente a cambiarsela ogni quindici giorni o in altri tempi ben definiti. È un problema e genera anche un costo. Tra chi se la cambia, chi non se la cambia e chi se la cambia male, alla fine si arriva in fondo a dover gestire un *helpdesk online*, che è estremamente costoso. Specialmente per le piccole amministrazioni è quasi improponibile la gestione di un *helpdesk* che supporti l'utente quando gli hanno sottratto una *password* o quando non se la ricorda.

È un sistema che ha valore aggiunto per il cittadino e per l'interlocutore pari a zero e che alla pubblica amministrazione, alla banca o al *service provider* costa mille. Sono costi infrastrutturali che alla fine producono solo una percezione di scarsa efficacia presso il cliente, di complicazione nell'uso del servizio, di disaffezione per l'uso dei canali a distanza. Dopo quattro o cinque volte che si cerca di barcamenarsi con il mezzo codice INPS che è pervenuto e con l'altra metà giunta per posta, ma finita nella casella della posta indesiderata: si instaura un atteggiamento per cui si va all'INPS direttamente. Si prende la macchina, si inquina, ci si presenta all'ufficio dell'INPS e si cerca di riottenere la credenziale, facendo perdere tempo a un impiegato che magari avrebbe questioni più importanti di cui occuparsi. Alla fine è un ostacolo al diffondersi della cultura della dematerializzazione sia dal lato dell'utente, sia dal lato del *provider* di servizi.

Per citare *Candide* e il migliore dei mondi possibili, che cosa potremmo desiderare ? Se vivessimo nel mondo dei nostri *desiderata*, noi vorremmo avere l'ubiquità, vorremmo avere l'indipendenza dallo strumento che adoperiamo e vorremmo accedere da postazioni remote anche pubbliche. *Why not* ? Perché bisogna per forza avere un'infrastruttura tecnologica da NASA in casa propria per poter accedere ai servizi ? Possono esserci anche *totem*, postazioni pubbliche a disposizione della popolazione meno abbiente o meno addottorata, che dalla postazione pubblica può esercire tutte le pratiche di tipo informatico.

Si deve anche poter lavorare su qualsiasi rete, sia essa ADSL, GPRS, 3G o WiFi. L'accesso alle strutture di servizio deve essere totalmente *network independent*.

Non dovremmo avere credenziali associate a un dispositivo. Ci sono molte banche che installano un certificato digitale nel PC dell'utente. Bene, ma quale PC ? Poi l'utente si reca in ufficio e il software nel PC dell'ufficio non c'è, ragion per cui non può accedere al servizio.

Non sono questioni da poco, perché limitano il campo rispetto all'ubiquità. Si deve poter lavorare dappertutto e con qualsiasi tipo di strumento si abbia a portata di mano. Possibilmente non si dovrebbe installare *software* sul proprio dispositivo, perché installare un *software*

va bene, ma i *virus* sono *software* che a volte dolosamente qualcuno può far installare sulla macchina di un altro, ingannandolo con finte *e-mail*.

Si tratta di metodi più che conosciuti, ahimè, che consentono a un attaccante sofisticato di installare un *software* che fa i suoi comodi e non i comodi degli utenti. Se non dobbiamo installare nulla su un dispositivo, siamo tutti tranquilli.

Dobbiamo essere compatibili con dispositivi di autenticazione come quelli che abbiamo visto, ossia la cartucciera di dispositivi tecnici, e anche con il *software*, perché nel campo delle *password* da bruciare stanno entrando sul mercato molti *vendor* che le danno anche sul telefono mobile, sul telefonino.

Si può obiettare che abbiamo le carte. Sì, abbiamo le carte regionali dei servizi, che sono molto diffuse in alcune regioni e sono state prodotte in maniera massiva. Rammento i progetti in cui ho lavorato, in Friuli-Venezia Giulia, Lombardia e Sicilia. Ci sono livelli di diffusione della carta, che poi funge anche da tessera sanitaria, molto elevati, però pochissimi hanno ritirato presso le Poste, perché normalmente tale funzione veniva svolta, per la loro capillarità, dagli uffici postali, il PIN di attivazione dell'autenticazione, ragion per cui la carta serve solo per portarla dal farmacista e leggere il codice fiscale.

Uno strumento potente come un dispositivo connesso a un PC, quale il lettore di *smart card*, se non esiste tutta la filiera culturale relativa all'uso della carta e soprattutto alla distribuzione dei dispositivi, non serve a nulla. Difatti, una grossa campagna che è stata svolta in regione Lombardia è stata quella di poter distribuire i dispositivi di lettura della *smart card*, però è un processo molto lento, che riguarda una percentuale disarmante della popolazione che ha una tessera sanitaria regionale.

In un contesto di mobilità questi dispositivi ovviamente non si usano, perché si devono infilare da qualche parte e normalmente nessuno consente di introdurre nel proprio computer chiavette o altri oggetti che potrebbero essere fonte di pericolo. Ormai la sensibilità esiste. In molte aziende addirittura le porte cosiddette USB vengono disabilitate. Anche nelle aziende di comunicazione vengono totalmente disabilitate, perché rappresentano una delle porte da cui possono entrare falle terribili per il sistema.

Noi crediamo che i dispositivi cosiddetti non connessi, come la rastrelliera degli oggettini, siano preferibili per l'autenticazione rispetto a dispositivi connessi, perché si può lavorare tranquillamente dalla postazione dell'aeroporto, come dall'albergo, dal computer di un amico a casa sua o dall'ufficio. Ciò è abbastanza comprensibile, non occorre spiegare nulla. Sono dispositivi che vivono di vita propria e che non hanno bisogno di una connessione fisica con il PC. Sono ideali dal punto di vista dell'usabilità, però non sono distribuiti normalmente da chi attribuisce un'identità digitale, se non dal proprio fornitore di servizi. La propria banca ne distribuisce uno e un'altra banca un altro.

Le credenziali potrebbero essere attribuite a dispositivi non connessi anche a partire da carte a *microchip* sia bancarie, sia CNS/CRS/CIE. Attrezzando con pochissimo investimento gli ATM, cioè i bancomat e i postamat, con un'applicazione molto semplice, si può leggere una carta CRS, la carta tessera sanitaria a *chip*, e consegnare al cliente una credenziale da utilizzare in maniera *detached*, ossia non connessa agli strumenti. Vengono forniti *user ID* e *password* per un dato periodo, previa identificazione, e si dispone poi di un dispositivo che legge l'oggetto. Quando l'oggetto viene mostrato, si spiega all'utente come si può autenticare.

In questo contesto c'è un'evoluzione a livello internazionale, che, peraltro, è anche consolidata dal punto di vista sia teorico, sia pratico, e che concepisce il ruolo del *service provider* come distinto da quello dell'*identity provider*. Non è detto che chi fornisce l'identità e chi autentica siano lo stesso soggetto che deve fornire il servizio.

L'*identity provider*, che è ben descritto in alcuni documenti anche a livello europeo condivisi anche a livello di Commissione, è un'entità che può essere pubblica o privata – ce ne sono diversi esempi – che identifica in maniera rigorosa un cittadino, gli assegna credenziali digitali, gli fornisce un'identità digitale unica e riconoscibile sia dalla pubblica amministrazione, sia da altri privati, e garantisce i servizi di autenticazione.

Supponiamo che io mi debba collegare con la mia banca. La mia banca butta via tutto l'insieme di apparecchiature e di sistemi per la mia autenticazione e gira la mia sessione di collegamento all'*identity provider*, che può essere uno per tutte le banche o per tutte le pubbliche amministrazioni. L'*identity provider*, che svolge un mestiere ben preciso, separato da quello che svolgono tutti, con il ruolo di fornitore di identità, in quel momento parla con me, non con la banca o con la pubblica amministrazione, e mi fornisce grandi garanzie di riservatezza nel colloquio di autenticazione: mi identifica, poi rigira la sessione, ma in maniera trasparente per l'utente – in realtà, l'utente non se ne accorge nemmeno; crede di lavorare con la sua banca, ma di fatto parla con l'*identity provider* – e il *service provider*, quello che fornisce il servizio, riceve dall'*identity provider* una cosiddetta asserzione di identità, cioè un « oggetto elettronico » firmato totalmente invisibile per l'utente, che garantisce a chi fornisce il servizio che la mia identità è quella che io dichiaro di avere.

È chiaro che sarebbe necessario sviluppare, più che altro dal punto di vista della volontà organizzativa e industriale, tale divisione fra fornitori di identità e fornitori di servizio, secondo schemi e tecnologie che sono di mercato, ma non di mercato addirittura a titolo oneroso. Tutte le strutture di *open authentication* sono disponibili sul mercato dell'*open source*. Il progetto ICAR interregionale prevede che qualunque entità di una data regione possa identificare e fornire credenziali a un cittadino e che, con un protocollo di interconnessione, tale cittadino venga riconosciuto da qualunque altro ente federato con questa struttura di autenticazione.

Stiamo passando a illustrare l'ultima questione, quella dell'identità federata. Poiché i meccanismi esistono e sono assolutamente *Industry Standard*, ossia sono meccanismi già funzionanti, non è per nulla balzano pensare che anche a livello legislativo si promuova la nascita di strutture, di mercato, peraltro anche fra loro indipendenti, sia del pubblico, sia del privato, che, aderendo a un protocollo sia tecnologico, sia soprattutto di prassi per quanto riguarda le responsabilità legali, possano fornire l'identità digitale in modo che sia riconosciuta nel circolo più vasto di *trusting* possibile. Difatti, si parla di *circle of trust*: tutti coloro che hanno un dato protocollo per il riconoscimento e per l'assegnazione delle credenziali appartengono federativamente, nel senso che ciascuno riconosce l'altro, a un dato *circle of trust*.

Nel pubblico basterebbe utilizzare le strutture che hanno già una grandissima capillarità, come la struttura dei comuni o quella delle Poste italiane, non escludendo però nessun altro operatore, in modo da garantire la coerenza delle informazioni anche con il sistema di interscambio anagrafico.

Come sapete bene, la gestione dell'anagrafe è di titolarità del comune. Il Ministero dell'interno detiene l'INA l'Indice nazionale delle anagrafi, però l'anagrafe è di titolarità del singolo comune. Peraltro, il comune, ed è una questione curiosa, se ci pensiamo, è l'unica entità nella nostra nazione che può erogare un documento di identità senza visionare un altro documento d'identità. Se, invece, si va a chiedere il passaporto, viene richiesta la carta d'identità.

A questo punto emerge l'ultimo problema. Credo di avervi tediato il giusto, come si suol dire. Sarei molto felice, come operatore della sicurezza, se, riducendo enormemente i costi per i *service provider* e, quindi, anche per le pubbliche amministrazioni, e aumentando molto il livello

di confidenza dei cittadini, potessimo avere ciascuno di noi una chiavetta, un oggetto o una *password* di autenticazione che ci permettesse di andare dappertutto e di essere riconosciuti dall'entità che ci troviamo più facilmente a disposizione o che ci chiede il prezzo minore.

Per realizzare questo obiettivo occorre mettere in piedi un intervento di tipo normativo, che però è, a parer mio, norma di secondo livello. Le normative di primo livello esistono tutte. Sappiamo come viene effettuata la certificazione digitale. C'è DigitPA che svolge la vigilanza sulla PEC o sulle Autorità di certificazione. Non ci dobbiamo inventare un altro carrozzone deputato a gestire l'identità digitale. Semplicemente ci deve essere un ente di vigilanza e credo che DigitPA abbia questa funzione nel suo DNA e nella sua *mission* originaria.

Chiaramente chi fornisce identità digitale, poiché potrebbe anche fornire false identità, deve essere in grado di garantire una copertura fortissima, come i certificatori attuali. Occorre solo trasporre la normativa sulla certificazione digitale agli *identity provider* e, quindi, fornire garanzie assicurative importanti rispetto a errori od omissioni che potrebbero portare danni. I danni devono essere coperti a livello assicurativo e chi opera come *identity provider* deve disporre di capitali adeguati al rischio.

Concludo con un ultimo punto, che credo possa essere normato. Scusate, la mia ignoranza in materia legale è estrema, però credo che una norma anche di secondo livello potrebbe essere molto importante per consentire a tutti i singoli *provider*, che si accreditano secondo i protocolli che potrebbe stabilire la DigitPA delegata, di avere la disponibilità della consultazione presso i singoli comuni, dove si trovano le informazioni, attraverso un sistema in rete.

In tal senso, ritengo che l'INA-SAIA sia il sistema nativamente deputato per svolgere questo tipo di lavoro e fornire una risposta molto semplice: il documento è vero o è falso? Oggi come oggi, per ottenere un'identità digitale falsa o per aprire un *account* bancario sotto falso nome, senza poi rispondere delle conseguenze, perché lo si apre per compiere azioni di tipo truffaldino, ci vuole poco. Per esempio, se io ho una carta d'identità falsa, ben realizzata, posso presentarla a un ufficiale bancario, perché secondo la norma del Testo unico bancario e le norme dell'antiriciclaggio basta una carta d'identità, un documento ufficiale. Se la carta d'identità è falsa, io assumo un'identità falsa o addirittura l'identità di qualcun altro con una carta contraffatta.

L'ultima nota che ho inserito nella mia presentazione è che ritengo obbligatorio che ci sia un servizio che venga espletato dal sistema dei comuni, che è il titolare del dato anagrafico, per poter, di fronte alla richiesta telematica, chiedere non chi è il soggetto, che cosa fa e quanti figli ha, nulla di tutto ciò, ma il numero di carta d'identità rilasciata dal comune di Sesto San Giovanni e intestata a un dato codice fiscale per confermare l'identità oppure no. L'altro collegamento deve essere compiuto con una struttura che esiste e che funziona benissimo, quella del CED interforze, che conserva il *database* dei documenti smarriti e rubati.

Rafforzeremmo moltissimo i poteri di assegnazione delle identità sulla base di un documento solo se terremo molto in conto questa opzione, cioè il fatto di poter validare il documento in tempo reale e di validarne anche l'eventuale smarrimento o sottrazione, operazione facilissima perché se ci si collega al CED interforze si conosce benissimo se il documento è rubato o smarrito.

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

DEBORAH BERGAMINI. Grazie, dottor Magini. Io penso che lei abbia svolto una relazione interessante su uno degli aspetti chiave della difficoltà di sviluppare transazioni o comunque operazioni attraverso la rete, un problema di cui il nostro Paese soffre.

Io, per esempio, giro con una pagina che contiene tutte le mie *password* e tutti i miei numeri. Se me la rubano, sono rovinata. È chiaro che si pone proprio un problema di mancanza di sistema che poi determina costi assurdi, ma che soprattutto tiene lontane le persone. È difficilissimo oggi vivere in modo sistematico il rapporto con le transazioni o con le operazioni compiute a distanza. È un problema che, peraltro, tocca, secondo me, le fasce di età più avanzata della popolazione, perché funge da deterrente al ricorso a tali strumenti.

Trovo curioso che non si sia mai riusciti, considerato anche ciò che si determina in termini di costo, a sistematizzare questo ambito, che è primario. Sono d'accordo con lei sul punto.

Volevo porle, però, due domande. Se può rispondere, vorrei sapere che tipo di esperienze estere conosce. Lei ha accennato molto rapidamente al fatto che questa entità dell'*identity provider* è già stata testata in altri Paesi. Le chiedo se ha esperienza del fatto che questa mancanza di sistematizzazione sia un problema cronico del nostro Paese o se sia, invece, proprio un problema generale. In quel caso ovviamente esso richiederebbe operazioni di altra natura, sovranazionali.

In secondo luogo, lei ipotizza nella sua visione uno o più *identity provider* e sostiene che bisognerebbe identificare entità che, dotate di strumenti opportuni, possano certificare le identità digitali e, quindi, fungere da intermediari non percepiti fra le due parti.

Quando all'inizio parlava di *identity provider*, io pensavo che lei concepisse nella sua idea una sorta di *Authority* dell'identità, un ente terzo, ovviamente pubblico, che si incaricasse di questo compito. Poi ho capito che lei ha, invece, in mente uno o più operatori in questo ambito che sono già *incumbent*, cioè già esistenti, e che possono utilizzare la loro rete per gestire il servizio.

In quel caso, come funzionerebbe ? Ogni società deciderebbe liberamente di appoggiarsi a questo o all'altro *provider* ? Grazie.

VINCENZO GAROFALO. La ringrazio, dottor Magini. Noi tutti cerchiamo di andare in una direzione, che è quella di usufruire di servizi telematici e di utilizzare al meglio strumenti che ci consentano di risparmiare tempo.

Buona parte della sua relazione, almeno il 70 per cento, ha sottolineato quali sono oggi i fattori che generano grande diffidenza nell'utilizzo di questi sistemi; una diffidenza che riguarda soprattutto le persone anziane, ma che in ogni caso condiziona anche chi vuole utilizzare o utilizza questi strumenti.

Noi abbiamo sempre affermato che la libertà dell'utilizzo di internet, per esprimersi genericamente – non sono un grande esperto, ma sono un utente che tende a utilizzare internet il più possibile – libertà che difendiamo e che più volte è stata oggetto di discussione, può diventare, però, un'arma veramente dannosissima, che, anziché incoraggiare, accentua la diffidenza nell'utilizzo della rete.

Se ogni giorno calcolassimo quanti tentativi vengono messi in campo per rubare l'identità di ognuno di noi, come lei ha affermato, utilizzando anche il nome di *provider* sicuramente affidabili, rimarremmo impressionati. I fornitori di diverse carte di credito invitano i propri utenti a prestare attenzione, ricordando loro che essi non inviano richieste di conferme via *mail*, ma effettuano soltanto telefonate.

Lei ha parlato anche dell'utilizzo del telefono. Personalmente sono stato impegnato la settimana scorsa almeno per un quarto d'ora a fornire dati che poi venivano registrati per un contratto telefonico. In un quarto d'ora si perde anche la voglia di stare al telefono. Ritengo che sia molto importante risolvere al più presto possibile il problema dell'identità informatica unica. Temo che più avanti andremo, più ciò sarà complicato e più sarà facile che si abbia poco piacere a praticare le strade dell'innovazione, perché alla fine subentrerà il

classico ragionamento per cui è meglio recarsi all'ufficio postale e compiere l'operazione direttamente, anche se ciò non rappresenta la scelta migliore.

Le chiedo se, oltre a quanto detto riguardo alla direzione da seguire, può fornirci separatamente anche una proposta che noi possiamo effettivamente sviluppare e studiare, avvalendoci anche della collaborazione di altri organismi e di chi è in grado di aiutarci a risolvere questo problema. Probabilmente non lo risolveremo in maniera definitiva, perché sappiamo che c'è chi studia continuamente come frodare, però in ogni caso non avremo più il *notes* o il cellulare e tutti i sistemi che ognuno di noi utilizza.

La collega che tiene tutto in un foglio è bravissima. Probabilmente, se si stilasse l'elenco di tutti i *provider* nei confronti dei quali si desidera l'accesso, si scoprirebbe che sono tantissimi e che ognuno ha un sistema di *password* differente e ognuno porta l'utente a doversene inventare fantasiosamente una che non faccia parte del dizionario che ha citato.

La pregherei di fornirci il maggior numero possibile di soluzioni praticabili perché altrimenti rischiamo di proseguire nel mantenere questo stato di diffidenza e probabilmente di alimentarlo.

PRESIDENTE. Pongo anch'io alcune domande, premettendo a scusante la mia poca dimestichezza con la materia, e metto insieme più questioni che stiamo affrontando.

Noi abbiamo discusso in Aula alcune mozioni e anche nel decreto semplificazioni c'è un articolo sull'Agenda digitale 2020, cioè sulla diffusione della banda larga e ultralarga. Tali mozioni sono state votate e abbiamo tenuto anche alcune audizioni di operatori delle telecomunicazioni nelle settimane scorse.

Sarei curiosa di sapere da lei che cosa pensa delle posizioni, al di là della situazione particolare italiana, che si sono registrate su questo tema: la scarsa diffusione dell'utilizzo da parte dei cittadini dei sistemi *e-commerce* e di accesso alla pubblica amministrazione è dovuta a un problema di rete e soprattutto di infrastrutture o a un problema di alfabetizzazione e di complicazione dell'accesso ?

Su questo tema si è svolta una discussione. È chiaro che un aspetto non esclude l'altro, perché l'infrastruttura è rilevantissima, ma io, per esempio, mi sono formata l'idea, approfondendo, che forse in questo momento la, pur inadeguata, nostra rete è comunque sottoutilizzata rispetto alle potenzialità per un deficit di alfabetizzazione, di semplicità, di sicurezza e di timori. Questa è la prima domanda.

La seconda è una curiosità. Lei ci ha mostrato diversi sistemi di accesso, con *password* e *username*, con il *token*, con la tesserina, che hanno diversi livelli di sicurezza. I diversi fornitori di servizi, i soggetti che lei ci ha elencato, quali aziende sanitarie, servizi privati, aziende private e servizi bancari, come scelgono un sistema piuttosto che l'altro ? Evidentemente alcuni sono più sicuri o meno sicuri. Sono liberi di scegliere quello che vogliono e, in questo senso, ne rispondono poi ?

Un cittadino che ha usufruito di un servizio bancario – porto un esempio, probabilmente sbagliato – col sistema di *password* e *username* è meno sicuro di un cittadino che ha, invece, un sistema con la *password* che si brucia ? Tale istituto bancario risponde, nel caso, di un eventuale danno al cittadino ? Chi tutela il consumatore rispetto a una scelta che mi sembra di capire sia commerciale e assolutamente autonoma da parte di chi fornisce il servizio ?

Passo all'ultima domanda. Mi scuso ancora per l'imprecisione, ma sono curiosità che mi sono venute ascoltando la sua relazione. L'auspicio, come ricordava il collega Garofalo, è capire che cosa si può fare. Mi sembra che il mondo ideale sarebbe quello di entità di *identity provider* che forniscano a ogni cittadino un sistema di *password* e di sicurezza per accedere a tutti i servizi.

Per arrivare a questo punto mi pare che le tecnologie esistano. Che cosa manca, dunque ? Occorre un intervento

legislativo, ma di che tipo ? Nelle sue note si afferma che vanno stabilite regole di interoperatività, di livelli minimi di servizio, di vigilanza e un servizio di validazione. Questo serve per far funzionare, se non ho capito male, l'*identity provider*, ma perché esso cominci a esistere e venga creato occorre a monte un intervento legislativo che lo imponga oppure no ?

Do la parola al nostro ospite per la replica, precisando che abbiamo poco tempo, perché in questo momento è iniziata l'Aula.

MARIO MAGINI, *Esperto di sicurezza informatica*. Rispondo rapidamente, prima di tutto, nell'ordine, all'onorevole Bergamini. Questo tipo di infrastrutture è descritto perfettamente a livello tecnico. Esse sono accettate dall'Unione europea e sono condivise anche da molti *incoming identity provider*, che ancora non sono *incumbent*, ma che stanno per entrare sul mercato.

Porto un esempio, secondo me splendido, realizzato in regione Emilia-Romagna con la tecno-struttura Lepida. Si tratta di una società *in-house* della regione che ha messo insieme un sistema che si chiama FedERa, un sistema federato per cui tutti i comuni dell'Emilia-Romagna possono fornire un'identità digitale al singolo cittadino, che è totalmente intercambiabile: se un cittadino di Castelfranco dell'Emilia si fa rilasciare l'identità digitale a Castelfranco con questo sistema federato e poi va ad autenticarsi sul comune di Reggio Emilia – parlo di casi specifici, perché sono andato a validarli, essendo l'unica esperienza di larga diffusione – lo può fare.

Non ci dobbiamo inventare l'acqua calda. Il sistema di *identity provider* funziona, è standard di mercato e non occorre normare più di tanto, anche perché i protocolli esistono. Non voglio entrare nel tecnico, ma c'è un linguaggio che si chiama *Security Assertion Markup Language* (SAML), ben noto nel nostro mestiere, un sistema di asserzioni con un protocollo condiviso che tutti gli *identity provider* possono scambiare con i *service provider*, che è impostato esattamente nella stessa maniera. Questo tipo di asserzione può essere ricevuto da chiunque.

Un'altra realizzazione importante è quella del GARR, il sistema della ricerca scientifica italiana a livello interuniversitario, che funziona esattamente secondo questo protocollo.

Io credo che dovremmo promuovere, più che normare, la nascita degli *identity provider* e con ciò vengo anche a una parte della risposta al Presidente. Più che normare dobbiamo definire un quadro in cui è auspicato incoraggiare, da un punto di vista legislativo, il formarsi di entità qualificate e delegare all'*Authority*, che è DigitPA – non ne vedo altre in Italia che possano occuparsene – la stesura delle norme tecniche per quanto riguarda i requisiti di sicurezza, esattamente come è stato fatto per la certificazione digitale.

Tutto sommato ritengo che sia più un problema industriale che politico legislativo. Il problema esiste nella misura in cui tutta la pubblica amministrazione potrebbe essere non incoraggiata, ma quasi costretta, con i tempi giusti di attrezzaggio, a utilizzare i servizi di identità digitale federati. È premiante, però, per la pubblica amministrazione, e immagino che in tal senso rientriamo nella norma, che l'utilizzo di strumenti federati venga valutato come virtuoso, con tutte le premialità del caso, nella misura in cui dismetta sistemi di autenticazione propri e aderisca a un sistema federato, uno qualsiasi, purché certificato da DigitPA. Non possiamo porre su piani diversi entità pubbliche e private. I certificatori digitali sono tutti i privati in Italia o quasi.

Riprendendo brevemente il discorso sulle operazioni, ci sono migliaia di attacchi, di cui pochissimi vanno a buon fine. Quei pochi causano un gran rumore, ovviamente, ma ci sono milioni di operazioni. Oggi disponiamo anche dei dati ABI sulle transazioni elettroniche e di *e-commerce*, che stanno vedendo uno straordinario sviluppo in Italia, collegato anche con il *mobile*.

Di rete ce n'è anche troppa rispetto a questa materia. È chiaro che rispetto alla

distribuzione di contenuti digitali in video e audio, cioè ai nuovi metodi alternativi di distribuire contenuti, siamo un Paese svantaggiato, anche se sempre a macchia di leopardo, perché nelle metropoli dove c'è elevata densità di utenti ciò funziona bene o benino, però in merito non ho una competenza specifica. La banda larga, come percepita dall'utente, si può rivelare, a seconda dei casi, efficiente o non efficiente, ma per quanto riguarda una transazione finanziaria o la presentazione di una DIA a una pubblica amministrazione, basta il *modem* del 1995. Non c'è bisogno di avere infrastrutture di banda larga particolarmente performanti.

Rispondendo alla vicepresidente, probabilmente il problema si divide 90 a 10, ossia è un problema di infrastrutture, ma anche di abitudine, soprattutto della pubblica amministrazione, ma anche dei grandi *provider*, a lavorare in questo modo.

Un intervento di carattere generale e forse anche normativo potrebbe essere quello di imporre alla pubblica amministrazione di comunicare qual è l'*identity provider* con cui è federata e di buttare via tutto il ciarpame di autenticazione e di distribuzione di *password* e di raccomandate. Io credo che solo nel comune di Roma si consumi una quantità industriale di risorse per distribuire le *password* che servono per andare a pagare una multa. A che cosa serve andare a pagare una multa con una *password* essendo il pagatore? Non è detto che il pagatore debba coincidere con il soggetto che ha commesso l'infrazione. Se c'è un numero di multa, la si deve poter pagare con la propria carta di credito, come soggetto pagatore che non necessariamente coincida con il soggetto debitore. In alcuni casi adoperiamo il cannone per sparare alle zanzare.

Se ci fosse una struttura che fornisce un'identità digitale basata su due o tre strumenti che non sono fra loro alternativi, cioè un *user ID* e una *password* per accedere ai servizi tranquilli, per esempio per vedere quanti punti di Mille Miglia, nonché il *token* o la *one-time password* per servizi più complessi, e una conferma via telefono della transazione, per esempio, con un SMS – il metodo più efficace per evitare gli « uomini nel mezzo » (Man in the middle) – per servizi ancora più complessi, il sistema potrebbe funzionare.

Non c'è nulla che debba essere normato. Le tecnologie crescono, perché la pericolosità degli attacchi cresce e crescono i livelli tecnologici di risposta, ragion per cui non credo che si debba compiere alcun intervento di tipo normativo sulla tecnologia. Quando l'abbiamo compiuto, abbiamo sbagliato, perché la normativa sulla firma digitale è stata riscritta dieci volte e ancora presenta caverne di ambiguità non banali.

Non dobbiamo andare a normare le tecnologie, ma dobbiamo stabilire quali sono le tecnologie standard. La Commissione europea e gli organismi deputati per la firma digitale hanno stabilito regole, strumenti di uso e oggetti informatici di costo vicino allo zero, perché sono distribuiti in *open source*: adoperiamo, dunque, i *framework compliant* con la normativa europea e favoriamo che sorgano *identity provider* riconosciuti, senza voler compiere favoritismi, il che sarebbe una stupidaggine.

Io sono convinto che se, ad esempio, Poste italiane e l'Ancitel, che ha la gestione dell'INA-SAIA con i comuni, e magari un paio di grandi banche, quelle che hanno il maggior numero di utenti, si consorziassero e venissero incoraggiati a formare un consorzio che trova remunerazione dall'esercizio dell'attività, il sistema funzionerebbe.

È chiaro che il *service provider*, anche quello pubblico, come l'INPS, ha bisogno di una remunerazione. Io non so quanto spenda l'INPS per la gestione dell'identità digitale, sia nella distribuzione, sia nell'autenticazione. Secondo me, è una cifra importante.

Si dovrebbe imporre a un ente pubblico di dismettere tutta quella parte, su cui si eseguiranno le autenticazioni e che genera un costo, potenzialmente cessante, enorme per la pubblica amministrazione. All'in-

terno di questa valutazione, che deve essere selettiva, di costi cessanti per le singole amministrazioni, potremmo introdurre il costo riveniente, che sarà un decimo di quello cessante, per l'utilizzo di servizi di terzi, privati o pubblici che siano. Si procederebbe a gara, come sempre. Spero di aver risposto sulla libertà di scegliersi il *service provider*.

La tutela del consumatore è importantissima e in questo momento è affidata a contratti *one-to-one* fra il consumatore e il suo *service provider*. Chi proteggerà questi contratti, secondo voi ? Hanno sempre ragione la banca o l'ente che hanno fornito lo strumento.

PRESIDENTE. Almeno su questo punto lei ritiene che occorra un intervento normativo ?

MARIO MAGINI, *Esperto di sicurezza informatica*. L'intervento normativo potrebbe essere di questo genere, ossia che il cosiddetto trasferimento di responsabilità sia a carico di questi IDP, i quali si assumono con una bella polizza assicurativa i rischi di *refund* delle eventuali transazioni dolose. È un problema loro, perché hanno identificato male la persona. La banca ha svolto il suo lavoro, perché le è arrivata l'autenticazione.

Così facendo, toglieremmo un problema a tutti, anche al cittadino, perché l'*identity provider* che ha consentito la transazione dolosa si vedrebbe ripagato immediatamente dall'assicurazione.

Forse rientriamo in un regime un po' troppo liberista da questo punto di vista, almeno come indirizzo, ma ci sono entità che sono assicurate per i danni che causano. Attualmente, se a lei sottraggono denari in una banca possono risponderle qualunque cosa, perché detengono loro i *log* della transazione e lei non li ha, la banca ha la registrazione del colloquio e lei no. Il consumatore in questo momento è in balia del suo fornitore di servizi.

Su alcune questioni, come il bancomat, esiste un Fondo interbancario di tutela dei depositi, un fondo comune che serve per rifondere i furti; però sicuramente si tratta di casi limitati.

Se, per esempio, viene sottratta una credenziale digitale e si compie un movimento di 500 euro da una carta a un'altra che non era quella vera di destinazione – se leggete i giornali, vedrete che è successo poco tempo fa – non viene restituito nulla, perché l'utente ha custodito male le credenziali. Non può dimostrare di averle utilizzate bene, essendo l'autenticazione stata svolta dal cittadino o da un terzo attore fraudolento venuto in possesso delle credenziali.

PRESIDENTE. La collega Bergamini aveva chiesto come funziona l'*identity provider* negli altri Paesi.

MARIO MAGINI, *Esperto di sicurezza informatica*. Negli altri Paesi le strutture dell'*identity provider* non sono normate, non c'è una norma. Sono descritte tecnicamente nei *draft* internazionali, ragion per cui sono norme *de facto*, norme industriali. Sono identiche sicuramente in tutti i Paesi dell'area euro e dell'Europa allargata, ma si stanno diffondendo anche negli altri Paesi.

Nell'ultimo convegno cui ho partecipato c'erano il direttore dell'informatica della Repubblica austriaca, nonché personaggi del NIST americano. Si tratta di procedure *in itinere*, ma convergenti su questo esatto protocollo di lavoro. Se lavoriamo su questo protocollo, non agiamo come è stato fatto in Italia con la posta certificata (PEC). Abbiamo creato un nostro oggetto, bellissimo, per l'amor di Dio, ne sono un cultore, però è un po' un *monstrum*, perché non è stato strutturato secondo standard riconosciuti a livello europeo e adesso dobbiamo compiere operazioni di adattamento. Se, invece, ci muoviamo su operazioni di *identity provisioning* omogenee non tanto ai dettami dei regolamenti, quanto a quelli delle norme tecniche a livello ISO Standard europeo, ci adeguiamo facilmente.

Ciò sta avvenendo molto rapidamente in Europa a livello di organismi di ricerca,

mentre il settore finanziario offre una credenziale uno a uno. Ci sono interessi fortissimi da parte dei venditori di soluzioni tecnologiche che le vogliono vendere a ciascuna banca. Se le compagnie che vendono sistemi di sicurezza trovano solo un *identity provider*, due o tre in Italia, come le Poste, l'Anci e un altro privato, a chi vendono ? Non c'è l'interesse dei *vendor* a promuovere l'interoperabilità.

PRESIDENTE. Ringrazio il dottor Mario Magini, esperto di sicurezza informatica, per la sua relazione e per il documento depositato, di cui autorizzo la pubblicazione in allegato alla seduta odierna *(vedi allegato)*.

Dichiaro conclusa l'audizione.

La seduta termina alle 15,15.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI ESTENSORE DEL PROCESSO VERBALE

DOTT. VALENTINO FRANCONI

Licenziato per la stampa il 6 giugno 2012.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO