coordinamento per permettere di eliminare il cosiddetto *digital divide*, soprattutto sul discorso infrastrutturale e sulle reti, a proposito del quale oggi siamo chiamati a rispondere ai quesiti che la Commissione ci ha posto.

In preparazione dell'incontro sulle tematiche che sono state sviluppate all'interno dell'Agenda digitale, è stato definito un rapporto che verrà presentato dalle regioni nel gennaio prossimo. Si tratta di un rapporto sull'innovazione in cui c'è una parte specifica sulle reti e sulle infrastrutture.

Noi abbiamo a disposizione un documento di sintesi che è stato presentato come memoria per l'audizione odierna e che è stato approvato in Conferenza. Esso delinea tre tematiche fondamentali, che sono state poste nelle richieste di contributo che le regioni potevano fornire sulla tematica dell'identità digitale.

Individuiamo un percorso molto importante che le regioni e il Governo devono svolgere per permettere agli utenti di avere effettivamente a disposizione strumenti che facilitino enormemente la fruizione dei servizi in modalità informatica.

Abbiamo anche individuato i temi della sicurezza relativamente alle reti di telecomunicazione. Una delle priorità consiste nell'individuare soluzioni tecnologiche, amministrative e normative perché vengano identificate le migliori soluzioni per la sicurezza delle reti.

Abbiamo svolto anche un intervento in cui siamo stati chiamati a essere ascoltati sulla tematica del *cloud computing*.

Cederei, pertanto, la parola al rappresentante dello *staff* tecnico del CISIS, dottor Andrea Nicolini, il quale svolgerà uno scenario sintetico su queste tre tematiche.

Rimarremo poi a disposizione su domande specifiche alle quali i rappresentanti delle regioni, in questo caso della regione Sardegna e della regione Emilia-Romagna, potranno fornire risposte più puntuali con riguardo al tema della sicurezza delle reti e del *cloud computing*. Tenete presente che sono già maturate all'interno dei territori regionali alcune esperienze che danno significatività alle risposte, nonché alcune sperimentazioni e alcuni sistemi che sono già in atto.

Ricordo ancora che anche la regione Piemonte ha lavorato su questo documento, che poi è stato approvato dalla Conferenza, il quale conferisce significatività alle azioni che le regioni nel loro insieme e nel loro coordinamento hanno identificato come più proprie.

Do la parola ad Andrea Nicolini.

ANDREA NICOLINI, *Consulente del Centro interregionale per i sistemi informatici, geografici e statistici (CISIS)*. Buongiorno. Ringrazio per l'audizione. Vorrei semplicemente delineare da un punto di vista tecnico i contenuti del contributo che abbiamo fornito e che ritrovate anche, come ha ricordato giustamente la dottoressa Pasetti, nella sintesi del rapporto che vi abbiamo lasciato come *memorandum*.

Le regioni rispetto ai tre temi hanno investito moltissimo sull'identità digitale, in piena sinergia con il livello centrale e, in particolare, con i diversi soggetti istituzionali che si sono occupati della definizione del sistema dell'identità digitale. Mi riferisco, in questo caso, all'ex CNIPA, poi diventato DigitPA e ora prossimo a diventare Agenzia per l'Italia digitale, con il quale abbiamo sviluppato il sistema GFID per la gestione dell'identità digitale a livello federato nazionale.

Quindici o sedici regioni hanno investito nella realizzazione di sistemi regionali che si basano sull'utilizzo di diversi strumenti per l'identificazione digitale. In questo momento riteniamo ancora leggermente carente la normativa sulla possibilità per gli enti del territorio di utilizzare strumenti più *user friendly*, come, per esempio, le *one-time password* utilizzate comunemente dai sistemi bancari, per consentire a tutti di poter fruire di servizi digitali in sicurezza con la propria identità.

Le regioni hanno utilizzato tale sistema per il fascicolo sanitario elettronico e per l'accesso ai portali. Alcune regioni, come il Friuli Venezia Giulia, l'hanno utilizzato per la carta carburante, ossia per la de-

tassazione dei cittadini in prossimità del confine. La regione Lombardia ha compiuto un investimento.

Oggi come oggi, sono oltre 20 milioni le carte regionali dei servizi distribuite, di cui circa il 50 per cento sono attive e utilizzate da cittadini comunemente nell'erogazione di servizi *on line* con la pubblica amministrazione.

Ovviamente è interesse delle regioni aumentare questo parco di servizi e di strumenti a disposizione dei cittadini e, nel limite del possibile, cercare di raggiungere il più presto possibile la totalità dei cittadini.

In questo senso le regioni sono state molto favorevoli all'unificazione del Documento unificato con l'Agenda digitale, che ha riguardato carta d'identità, carta regionale e carta nazionale dei servizi, anche se tale processo richiede, per essere completato, dieci anni. Noi cercheremmo, come regioni, di accelerare il più possibile il raggiungimento della totalità dei cittadini.

Sull'identità digitale non tutto è ancora concluso, ma molto è stato compiuto, ragion per cui siamo contenti a livello regionale. Avremmo bisogno, però, ed è un appello che abbiamo rivolto ripetutamente ai Ministri che abbiamo incontrato, che le amministrazioni centrali uniformassero a loro volta i propri servizi all'identità digitale e che il cittadino potesse accedere in modalità uniforme ai servizi sia del territorio, ossia di regioni, comuni e province, sia a quelli dell'amministrazione centrale.

Oggi, purtroppo, nella maggior parte dei casi il cittadino deve utilizzare sistemi differenti. Pensiamo all'INPS, all'Agenzia delle entrate e ad altre realtà che richiedono sistemi di identità diversi rispetto a quelli istituiti e creati dalle regioni.

Per quanto riguarda la sicurezza nelle reti, le regioni hanno lavorato in una logica di sistema pubblico di connettività e di cooperazione da quando esiste il CAD. Dal 2005 hanno attivato i centri di sicurezza regionali, CERT. Undici regioni hanno il CERT attivo anche per il territorio, non solo per l'ente regione e, quindi, supportano in sussidiarietà comuni e province del proprio territorio.

Le regioni hanno investito moltissimo sulle infrastrutture di connettività. Il *digital divide* sul territorio negli ultimi due anni è sceso dal 9 al 5 per cento, un calo di quattro punti in percentuale determinato anche in gran parte dagli investimenti sul territorio compiuti dalle regioni e dalle province autonome, relativi anche all'ultimo miglio, per favorire il superamento del *digital divide* per i cittadini, per le imprese e per le pubbliche amministrazioni.

Da questo punto di vista, per le regioni sarebbe fondamentale che avvenisse una piena attuazione a livello centrale del CERT, il centro di sicurezza nazionale, che, nel passaggio fra l'ex DigitPA e l'attuale Agenzia per l'Italia digitale, sta un po' soffrendo della mancanza, negli ultimi dodici mesi, di una politica forte e chiara. Le regioni richiedono assolutamente di procedere il più rapidamente possibile a sollecitare in questo senso anche il Governo.

Per quanto riguarda, invece, il *cloud*, la situazione è meno consolidata. Ci sono sei o sette regioni che hanno investito in *data center* regionali in logica *cloud*. Più che di soluzioni *cloud*, io parlerei, però, di paradigma *cloud*, nel senso che hanno investito nello sviluppo di infrastrutture e di servizi per le piattaforme e servizi, un intero *set* di infrastrutture dedicato a erogare servizi finali.

In questo senso gli investimenti effettuati dalle regioni per raggiungere il miglior livello di sicurezza auspicato dovrebbero andare nella direzione di una federazione nazionale di *cloud* e di *data center* che consentirebbe di garantire il servizio in qualunque condizione e di ottenere il maggior ritorno degli investimenti compiuti, sposando una logica, una piattaforma, un paradigma di questo tipo.

Sempre nella logica SPC, il sistema pubblico di connettività e cooperazione, creato con CAD e sviluppato in logica federata policentrica e non gerarchica, è più aderente all'organizzazione dello Stato e del territorio con le amministrazioni a

più livelli. La federazione è, dunque, la forma che meglio consente di assecondare le diversità sul territorio.

Con le informazioni e le note tecniche mi fermerei a questo punto. Se ci sono domande, sarò a disposizione. Lascio ora la parola ai colleghi.

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

JONNY CROSIO. Grazie, presidente, mi scuso del ritardo. Oggi non c'è una grande presenza in Commissione, anche perché trattiamo un tema specifico. Siamo in pochi a interessarcene, essendo la nostra una Commissione che si occupa di molti temi, anche di trasporto. Io dovevo dividermi tra TG Parlamento, che voleva sapere dell'audizione, e l'Aula.

Avrei una domanda. Il vostro contributo all'Agenda digitale del Paese è di giugno 2012. Non mi sembra di averne letto nell'ultimo provvedimento passato in Aula la settimana scorsa. Non credo di riferire una notizia illegale se affermo di aver già visto il documento. Non l'ho avuto di straforo. È un documento importante perché apporta un contributo all'Agenda digitale del Paese, che temo non sia stato preso in considerazione, se non in parte.

Io credo che voi siate uno degli anelli intermedi di tutto il sistema di sicurezza delle reti. Abbiamo visto sia con la Polizia postale, sia con altre realtà che su questo tema bisogna cercare di lavorare a favore di una soluzione sempre più centralizzata.

Io non sono, per ragioni politiche, a favore della centralizzazione e non sono propenso a riportare allo Stato competenze su alcunché, ma credo che su questi temi non si possa fare altrimenti, perché il frazionamento porta alla disperazione e alla miseria per quanto riguarda le reti.

Mi interesserebbe conoscere un vostro punto di vista. È una domanda che ho posto anche a chi vi ha preceduto.

Noi abbiamo certamente capito che nel nostro Paese, come in diversi Paesi europei, manca la base giuridica per poter fronteggiare determinate situazione di *cyber crime*. Il legislatore e il Governo – se ne occuperà qualcun altro nella nuova fase politica: io nel prossimo Governo sarò all'opposizione – dovranno metterci mano. Tale operazione porterà al fatto che nel nostro Paese dovremo, se vogliamo avere sicurezza nelle reti, svolgere alcune riflessioni sulla *privacy*.

Non possiamo pensare di avere un sistema più *strong* per quanto riguarda l'identificazione e sposare ancora la filosofia molto accattivante della « rete libera per tutti ». Dobbiamo investire in sicurezza seriamente. È chiaro che questo significherà creare veramente le condizioni per cui la *privacy* dovrà essere un po' ridimensionata.

Dal vostro punto di vista, voi, che rappresentate la parte amministrativa, sareste disposti a recepire questo aspetto in funzione della maggiore sicurezza ? Se non riusciamo a superare questo *empasse*, sarà molto difficile garantire più sicurezza. Più che di voi, ossia delle realtà regionali e amministrative, che comunque possono difendersi, noi siamo preoccupati, in modo particolare, del grosso problema del furto delle identità sui cittadini.

In base ai dati che ci vengono forniti sappiamo che il crimine sulla rete quest'anno ha avuto più PIL che la vendita di cocaina a livello mondiale. Noi siamo preoccupati, tutti i Paesi lo sono. L'Agenda digitale europea ci ha fornito alcuni riferimenti, che non possono essere disattesi. Tali riferimenti sono il preludio al fatto che forse sulla *privacy* qualcuno deve volare un po' più basso. Sarà un'operazione fattibile ? Che cosa ne pensate ?

PRESIDENTE. Do la parola ai rappresentanti della Conferenza delle regioni e delle province autonome per la replica.

ANDREA NICOLINI, *Consulente del Centro interregionale per i sistemi informatici, geografici e statistici (CISIS)*. Svolgo un brevissimo accenno alla prima parte della domanda relativa all'Agenda digitale.

Come regioni, noi abbiamo collaborato moltissimo nella fase della stesura del testo proposto dal Governo, che ha rece-

pito quasi tutte le nostre richieste di modifica. L'unico appunto che abbiamo mosso rispetto a tale documento è che manca un disegno attuativo dell'Agenda.

Va benissimo emanare la norma, capiamo benissimo che ci sono pochi fondi, però ci si sarebbe potuti concentrare, come avevamo consigliato noi, in una o due azioni Paese che potessero davvero cambiare il volto del sistema, per esempio passando con uno *switch-off* al digitale nella documentazione della pubblica amministrazione. Questo tema sarà materia di ulteriori confronti con l'Agenzia per l'Italia digitale e col nuovo Governo, quando sarà eletto.

Per quanto riguarda, invece, la domanda specifica sull'identità, la pubblica amministrazione, paradossalmente, è troppo sicura, e lo è a tal punto che i suoi servizi non vengono usati come dovrebbero, proprio perché richiedono livelli troppo alti di sicurezza. Effettuare un furto di identità su una *username* e una *password*, come nella maggioranza dei sistemi pubblici disponibili su Internet, presenta un grado di complessità molto basso. È molto facile compiere un furto di questo tipo.

Effettuare un furto di identità digitale con una carta d'identità digitale elettronica attuale o una carta regionale dei servizi, che necessita di un lettore con relativi *username* e *password* o di PIN e PUC di blocco e sblocco è molto più difficile. È più difficile ancora che per i bancomat, per alcuni aspetti. L'identificazione, al momento in cui si distribuisce lo strumento, è molto più forte. Nella pubblica amministrazione si dovrebbe identificare il cittadino in modo stringente e forte, mentre per le SIM e i bancomat non è così.

Per l'identità la sicurezza è, dunque, ancora più forte nella pubblica amministrazione. Paradossalmente, proprio il problema che la pubblica amministrazione ha per i propri servizi è quello di scendere di un livello e consentire una più facile fruibilità almeno per i servizi che non sono critici e che non riguardano informazioni riservate.

In questo senso esiste il progetto europeo STORK che lavora per facilitare – ora si è alla seconda versione del progetto – la possibilità di fruire facilmente di servizi in sicurezza sull'identità digitale transnazionale, fra più Paesi della Comunità europea. Da questo punto di vista, si abbassa, dunque, il livello.

Non a caso prima ho citato le *one-time password*. Per esempio, il CAD attuale identifica tre livelli di sicurezza.

Il primo, *username* e *password*, è il più basso e garantisce pochissima sicurezza di accesso.

Il secondo prevede *username* e *password* più *one-time password*, ossia l'utilizzo di un codice che può essere usato una sola volta. In questo senso noi spingiamo addirittura per non usare nemmeno le chiavette delle banche, per intenderci, ma la *one-time password* come strumento di controllo, come un cellulare. Tale operazione facilita enormemente l'utilizzo da parte dei più.

Infine, c'è il terzo livello, che prevede la *smart card* e il *chip* che deve essere a contatto con un lettore, oppure anche *contactless*, per identificare in maniera forte l'utente. Si arriva poi alle chiavi biometriche, che rappresentano l'ultimo livello in assoluto, una combinazione dei precedenti.

Più si alza il livello, dunque, minore è la fruibilità dei servizi da parte dei cittadini, ragion per cui bisogna trovare un giusto compromesso. Non ha neanche tanto senso puntare al livello più alto in assoluto per un'iscrizione all'asilo, per esempio, perché l'iscrizione all'asilo non deve richiedere livelli di sicurezza, ma deve essere facilmente fruibile da parte di tutti.

È difficile che un cittadino paghi la multa per me. È difficile che qualcuno attui un furto d'identità per pagare una multa. È molto più facile che si attui un furto di identità per fruire di servizi di agevolazione e di *benefit* normalmente legati a informazioni riservate, come il permesso per l'handicap. È più facile che con la pubblica amministrazione interessi rubare l'identità, fermo restando che per la

pubblica amministrazione il furto d'identità è ancora molto contenuto. Avviene per gli altri servizi erogati tramite la rete.

Da questo punto di vista, come pubblica amministrazione, a noi interessa lavorare in modo corretto con il Governo e con l'amministrazione centrale per individuare il giusto livello di sicurezza.

In merito alla sicurezza in generale, invece, noi siamo contrari alla centralizzazione sempre e comunque. Siamo molto favorevoli, invece, a un forte coordinamento centrale. A nostro avviso occorre un forte coordinamento centrale, mentre i servizi di controllo devono essere decentrati, perché è molto più facile controllare sul territorio.

Il controllo che sul territorio, oltre alle forze dell'ordine, possono effettuare le pubbliche amministrazioni, che hanno un contatto quotidiano con il cittadino, è molto maggiore di quello che può eseguire una pubblica amministrazione centrale. Penso all'Agenzia delle entrate, che ha le sue articolazioni sul territorio, ma non ha il controllo e il rapporto costante con il cittadino, come l'hanno invece le pubbliche amministrazioni sul territorio. Per la sanità un cittadino ha un'interlocuzione costante con la regione, con il comune o con la provincia, ragion per cui è molto più facile controllare la sua identità e gli strumenti utili.

FABIO PERNIOLA, *Rappresentante della regione Emilia-Romagna*. Buongiorno, sono l'ingegner Perniola e mi occupo di sicurezza informatica all'interno di Lepida SpA, la società *in house* della regione Emilia-Romagna.

Vorrei aggiungere un contributo basato sulla nostra esperienza a uno dei due temi che era stato sollevato. Su quello della *privacy* e sicurezza ha già ampiamente risposto Andrea Nicolini, in particolare per quanto riguarda la pubblica amministrazione.

In base alla nostra esperienza vorrei sottolineare d nuovo, al di là di quanto non sia già stato fatto, la necessità di una visione coordinativa di livello più alto per il cosiddetto *enforcement* delle regole. Ciò vale soprattutto dal punto di vista organizzativo.

Se da un punto di vista tecnico la decentralizzazione può presentare effetti di efficienza maggiore, anche in considerazione dell'esigenza di far dialogare diversi soggetti che appartengono alla sfera pubblica e privata. Nei casi che concernono le Autorità di Polizia giudiziaria e di Polizia delle comunicazioni il nostro coinvolgimento come rete regionale va di pari passo con quello degli operatori di comunicazione, ossia dei *player* nazionali. Molto spesso questi due mondi, al di là del dialogo sul livello tecnico, hanno difficoltà ad interagire. Confermo, dunque, l'esigenza dell'*enforcement* delle regole.

PRESIDENTE. Ringrazio i rappresentanti della Conferenza delle regioni e delle province autonome per essere intervenuti e per la documentazione depositata, di cui autorizzo la pubblicazione in allegato alla seduta odierna (*vedi allegato 2)* e dichiaro conclusa l'audizione.

Audizione di rappresentanti di ABI Lab.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza informatica delle reti, l'audizione di rappresentanti di ABI Lab.

Do la parola al dottor Pierfrancesco Gaggi per lo svolgimento della relazione.

PIERFRANCESCO GAGGI, *Vicepresidente di ABI Lab*. Grazie, presidente. Buongiorno a tutti. Come sapete, vi abbiamo trasmesso questa mattina una corposa documentazione, che io ora mi limiterò a riassumere brevemente. Abbiamo anche preparato un altro *dossier* con un po' di materiale, perché abbiamo un Osservatorio annuale dedicato proprio al tema della sicurezza e delle frodi informatiche. Pensavamo, pertanto, di lasciarvene copia.

Da quanto avrete già avuto modo forse di scorrere nell'intervento che abbiamo prodotto avrete certamente potuto verificare che il tema della sicurezza delle reti

per le banche è un tema centrale. Per noi la gestione sicura dell'identità rappresenta un punto fondamentale anche in termini di vantaggio competitivo per le banche nello sviluppo del *business*, perché è considerata un fattore determinante per garantire sicurezza al cliente.

Vi fornisco alcuni dati di riferimento. Ne avrete già acquisiti molti, ma aggiungo quelli che noi abbiamo raccolto e che raccogliamo annualmente. Secondo tali dati il canale Internet in banca è diffuso su un numero di *account retail* che nel 2011 è risultato superiore a 20 milioni. Di questi 13 milioni sono attivi e in costante crescita.

Naturalmente, stante il numero crescente di utilizzatori, c'è anche un aumento dei tentativi di frode, perché la criminalità guarda sempre con maggiore attenzione a questo fenomeno, che è ormai diventato di massa, ossia l'utilizzo del canale Internet.

La criminalità si sta spingendo sostanzialmente su due forme di tentativi, il cosiddetto *phishing* e il *crimeware*. Sulle modalità credo che avrete già raccolto molte informazioni. Tuttavia, espongo alcuni elementi su come vengono utilizzate queste forme nell'ambiente bancario.

A noi risulta che, con riferimento al furto di identità elettronica dei clienti, cioè alla sottrazione delle credenziali al fine di operare sul conto della vittima, il 94 per cento delle banche di un nostro campione, composto di circa 200 banche, quindi in sostanza 180 banche, ha dichiarato di aver rilevato tentativi mirati al furto delle credenziali di propri clienti.

A livello generale sul segmento *retail* si registra un aumento della perdita di credenziali rispetto all'anno passato, ma occorre precisare che l'efficacia dell'azione di contrasto da parte delle banche è tale per cui di fatto oltre il 98 per cento dei tentativi di frode non va in porto.

I casi in cui avviene il furto di credenziali che poi determina un caso di perdita di denaro è di un utente attivo ogni 2 milioni di accessi. Il dato è misurato in termini di numero di accessi.

Se misuriamo, invece, in termini di clienti attivi, si tratta di uno ogni 50.000. Siamo ancora su livelli fortunatamente più che accettabili, nel senso che abbiamo un'azione di contrasto della frode che riesce a frenare la quasi totalità degli attacchi.

Certamente, resta sempre quel « quasi », per cui alcuni clienti finiscono col sopportare non tanto una perdita – credo che siate già informati che tendenzialmente, nel caso di perdite economiche, cioè di una frode che abbia avuto successo dal punto di vista dei criminali, chi sopporta la perdita è sempre la banca e non il cliente finale – quanto l'essere invischiati in un noiosa pratica, che certamente lo colpisce. Di fatto, però, chi sopporta la perdita finale è la banca.

Ci risulta, invece – stiamo attivando un analogo osservatorio anche sul canale *mobile* – che sul canale *mobile* non ci sia ancora alcuna perdita di credenziali. Non c'è accesso non autorizzato ai servizi *mobile banking*.

Dal punto di vista normativo sapete che si sta via via accumulando una quantità di nuova normativa, perché la materia è alquanto nuova. Di conseguenza, anche la normativa di riferimento viene via via creata in questi anni. La Banca centrale europea ha emanato alcune direttive sull'utilizzo dei servizi *on line*, con Eurosistema, il che riguarda anche Banca d'Italia.

In particolare, è stata approvata ed è stata anche recepita nell'ordinamento italiano la direttiva europea sui servizi di pagamento, la *Payment Services Directive*. Tutte queste norme delineano modalità di utilizzo degli strumenti molto tutelanti nei confronti della clientela.

Su questo punto, se mi posso permettere un momento di riflessione, osservo che un eccesso di tutela nei confronti del cliente rischia di deresponsabilizzarlo. Una questione cui noi teniamo molto è quella di compiere molta formazione e comunicazione. Predisponiamo molto materiale che poi viene utilizzato dalle banche nel contatto con la propria clientela. Non possiamo pensare, però, che rendere

il cliente sempre e comunque indenne nei confronti di queste situazioni sia corretto.

Il nostro obiettivo non è quello di colpire il cliente, che va tutelato, ma bisogna pensare che tutte queste frodi avvengono sostanzialmente sul PC, che è uno strumento del cliente. Infondergli il senso della delicatezza dello strumento col quale si interfaccia, a nostro avviso, è un obiettivo importante. Bisogna stare attenti. Non è facile, ma bisogna trovare il modo per bilanciare la tutela del cliente con una sua azione sempre più responsabile e attenta.

Al di là della predisposizione dell'aspetto informativo nei confronti delle banche perché adottino tutte le normative, oltre che le modalità operative più tutelanti per le banche stesse e per la clientela, noi abbiamo aderito anche ad alcune iniziative a livello internazionale. Partecipiamo a molti *fora* – ne avete incontrato uno poco fa – e lavoriamo molto al contatto con la Polizia postale e delle comunicazioni, con l'Autorità garante della protezione dei dati personali, con il Ministero dell'economia e delle finanze e con DigitPA. Ci sono gruppi europei che seguono le tematiche delle frodi su Internet, di cui facciamo ovviamente parte.

Da questo punto di vista cerchiamo sempre di stare sulla frontiera dell'informazione a livello europeo. Abbiamo alcuni osservatori, che diventano però aspetti molto concreti. Non stiamo solo a confrontarci sui dati, ma attuiamo anche modalità di rapido intervento e di scambio tramite *e-mail* di informazioni.

Quando si ha il sentore che scatti una frode, scatta un pronto intervento. Abbiamo creato questo strumento, che chiamiamo osservatorio, ma che è una centrale di allarme tra banche, che si interfaccia con analoghe centrali di allarme all'estero. Ci scambiamo immediatamente alcuni dati ed elementi relativi alla frode in corso per far sì che, possibilmente, essa venga bloccata.

Ci sono alcuni progetti europei, dei quali peraltro siamo stati invitati a far parte, come il progetto « On line Fraud Cyber Centre » e il progetto europeo STORK 2.0 sull'identità sicura *cross-border*.

Da questo punto di vista, riteniamo di poter offrire alle nostre banche – noi siamo, come ABI Lab, un consorzio che, *a latere* di ABI, segue le tematiche della tecnologia, consorzio al quale partecipano 200 banche, praticamente tutte le banche principali; il livello dei rappresentanti di banche che partecipano ai nostri seminari e ai nostri lavori è molto ampio – non solo informazioni, ma anche strumenti concreti ai quali esse stesse partecipano.

Sulla base di questa nostra esperienza ci sentiamo di poter formulare alcune proposte di natura sia normativa, sia operativa. Mi dirigerei direttamente a questo tipo di proposte.

A nostro avviso, sarebbe importante – probabilmente è anche uno degli scopi di questa indagine – trovare il modo di regolamentare e sanzionare il reato di furto di identità elettronica e di inquadrare alcune modalità operative per lo scambio di informazioni dei dati proprio in caso di frodi informatiche tra i diversi soggetti interessati che non ledano la legittima aspettativa di tutela nel settore della *privacy*, ma che, allo stesso tempo, forniscano strumenti agili per chi deve tutelare l'aspetto sicurezza per scambiarsi informazioni sulle frodi in corso.

Dal punto di vista delle prospettive immediate noi siamo molto lieti dell'approvazione avvenuta di recente del decreto che è stato convertito, il cosiddetto decreto « Crescita 2.0 », il quale offre finalmente la possibilità di varare su scala nazionale i documenti di identità elettronica per i cittadini. È una vicenda che abbiamo seguito da anni con attenzione e che ora si avvia finalmente alla sua implementazione.

Ci sembra poi particolarmente importante che il contesto normativo nazionale possa essere indirizzato a definire alcuni strumenti giuridici che consentano alle banche di tutelare gli attributi identitari dei propri clienti, qualora vengano utiliz-

zati da soggetti terzi che partecipano all'erogazione dei servizi da parte delle banche.

Sappiamo che nelle transazioni bancarie il cliente vede la banca, ed è giusto che sia così, anzi noi siamo assolutamente gelosi di questo rapporto. Non vogliamo spossessarci o deresponsabilizzare le banche nei confronti della catena che sta a valle della banca. Tuttavia, dobbiamo tener conto che forse questa catena, che è piuttosto lunga, perché la banca si avvale di alcuni soggetti che la supportano nello svolgimento delle transazioni, oltre che sulla base di un rapporto contrattuale che lega tutta la catena, forse dovrebbe avere alcuni aspetti normati a livello proprio di normativa primaria che valessero per tutti coloro che si apprestano a fornire servizi in quel contesto, nel settore delle reti e, in particolare, dell'*e-banking*.

Dal punto di vista operativo sarebbe importante e utile fornire anche alcune indicazioni su queste modalità di condivisione delle informazioni. Non so se ciò debba avvenire a livello normativo primario o regolamentare, ma sarebbe bene che ci fosse una standardizzazione delle modalità di colloquio tra i soggetti che si devono scambiare le informazioni quando sono in corso le frodi. Forse sta più alle Autorità di polizia poter lavorare su questo fronte.

Ci sembra particolarmente utile anche la previsione di includere nella carta d'identità elettronica un certificato di firma digitale. Anche su questo tema ormai da alcuni anni abbiamo abbracciato tale possibilità di integrazione su uno stesso strumento dei servizi sia di natura bancaria, sia di riconoscimento dell'identità dal punto di vista istituzionale. Le banche avevano già i loro sistemi di riconoscimento dell'identità, ma vediamo con molto favore il fatto che ora si abbia una carta di identità elettronica che può essere arricchita di un certificato di riconoscimento digitale.

Passando rapidamente alle reti del settore bancario – immagino che alcune siano note – c'è la SWIFT, quella internazionale, che collega tutte le istituzioni a livello mondiale. Vi partecipano anche direttamente circa 150 banche italiane e indirettamente tutto il sistema bancario.

Noi abbiamo una rete nazionale interbancaria che vede la partecipazione di più soggetti, tra cui la stessa Banca d'Italia, le banche, le poste, numerosi consorzi e soggetti che svolgono attività di tipo applicativo per conto delle banche su questa rete.

C'è poi la rete del CBI, il Consorzio avviato dalle banche e dall'ABI alcuni anni fa. È un consorzio che si preoccupa di definire standard e di fornire la rete per l'interazione tra banche e clientela *corporate*.

Con riferimento alle statistiche che inizialmente avevo citato, osserviamo una crescita dei tentativi di frode anche nel settore *corporate*. La quantità è ulteriormente ridotta in termini di successo della frode rispetto a quanto avviene nel settore *retail*, tuttavia osserviamo casi anche nel settore *corporate*, a tassi del doppio rispetto a quelli che avevo citato per il settore *retail*.

Per quanto riguarda le nostre proposte, sono quelle che vi ho già citato. A questo punto, io riterrei di fermarmi. Non so se siete interessati alle tematiche del *cloud computing*, ma forse, se vogliamo avviare una interlocuzione, sarebbe più utile se aveste domande da porgere.

PRESIDENTE. Vi ringraziamo. Nelle sintesi delle azioni proposte penso ci sia un documento che avete scritto che sarà di grande utilità ai fini della conclusione di questa indagine.

JONNY CROSIO. Grazie, presidente. Vi ringrazio per la vostra relazione, che avremo modo di analizzare in maniera più compiuta. Credo che nell'ambito della sicurezza delle reti e, in modo particolare, della tutela del cliente voi siate forse i soggetti che stanno agendo di più, anche

perché giustamente parliamo di soldi e sui soldi non si scherza mai.

Per esperienza personale io ho avuto un caso di controllo sicurezza poco tempo fa, mentre stavo effettuando acquisti su *e-Bay*. Dopo il terzo acquisto – era una domenica pomeriggio, alle 16.30 – ho ricevuto una telefonata in cui mi si chiedeva se effettivamente stavo compiendo tali acquisti.

Mi ha fatto molto piacere – visto che mi occupo di sicurezza – ricevere questa telefonata, apparentemente molto invasiva nei miei confronti. Ho commentato con mia moglie che era un fatto eccezionale.

Peraltro, avendo compiuto forse un'operazione un po' maldestra, avevo la preoccupazione di aver compiuto un pagamento doppio, ma la signorina che mi ha interpellato mi ha chiarito subito anche questo dubbio. Per questo tema l'associazione bancaria e il sistema delle carte stanno contribuendo facendo molto.

Tuttavia, c'è un tassello che vi riguarda e che a noi interessa molto, quello della questione del furto d'identità. Sulla sicurezza in generale delle reti i grandi sistemi di sicurezza che devono interagire fra di loro vanno più che altro a tutelare determinate situazioni. Noi crediamo che il cittadino sia il soggetto più a rischio in questo momento e che il furto d'identità sia un fenomeno molto preoccupante.

Si registra la carenza dello strumento giuridico. La Polizia postale si lamenta per questo motivo. Ciò produrrà il fatto che il legislatore dovrà mettere mano alla questione, il che significa che – oggi l'ho chiesto a tutti gli intervenuti e continuo a chiederlo sistematicamente, perché è questo il problema – la *privacy* dovrà essere valutata probabilmente in altre condizioni, non dico con altre regole, ma con un'ottica diversa.

Voi dell'ABI come vedete questo tema ? Probabilmente dovremo essere più *strong* verso l'utente nel richiedere informazioni, le quali dovranno convergere in una banca dati o comunque in un servizio di banca dati che dovrà essere storicizzato. Sicuramente chi gestirà la *privacy* nel Paese non ne sarà felice, ma lo « scollinamento » è questo: o avere più sicurezza, o garantire la *privacy*.

Il legislatore dovrà decidere se indirizzarsi verso la sicurezza della rete, in modo particolare a tutela dei più deboli, dei cittadini che del furto di identità non si accorgono neanche, dal momento che il Paese soffre di un *digital divide* anche culturale, o se tutelare la *privacy*. Purtroppo, i dati sono questi.

Dovremo compiere alcune scelte e dovremo presentare alcune proposte di legge. Il nostro compito è questo. L'indagine alla fine deve arrivare a questo obiettivo. Io ho provato a metterci mano con alcuni colleghi, ma è difficile trovare il punto di equilibrio. Le banche che cosa ne pensano ?

PRESIDENTE. Do la parola al dottor Pierfrancesco Gaggi per la replica.

PIERFRANCESCO GAGGI, *Vicepresidente di ABI Lab*. Io credo di poter compiere un'analogia un po' ardita con quanto è avvenuto nel settore fiscale dell'acquisizione dei dati dei conti della clientela. Noi, come intermediari, siamo neutrali rispetto al fatto che ci sia una maggiore richiesta. Ci preme molto che ci sia tanta sicurezza.

Da questo punto di vista non siamo negativi rispetto alla richiesta di maggiori informazioni. Certo, il cliente deve essere informato, deve sapere che i suoi dati devono essere acquisiti. Da parte nostra vorremmo adottare sempre modalità poco invasive nei confronti delle procedure delle banche.

Una volta che ci si mette a lavorare per un obiettivo condiviso di garantire più tutela al cliente, come abbiamo fatto per l'apparato fiscale e per il controllo dei

dati, per il quale lo Stato ci ha chiesto di fornire determinate informazioni, noi ci attrezziamo. L'importante è che la finalità sia riconosciuta in uno strumento giuridico primario.

Da questo punto di vista, dunque, non siamo contrari all'iniziativa, anzi !

PRESIDENTE. Ringrazio i rappresentanti di ABI Lab per essere intervenuti e per la documentazione depositata, di cui autorizzo la pubblicazione in allegato alla seduta odierna (*vedi allegato 3)* e dichiaro conclusa l'audizione.

La seduta termina alle 16,05.

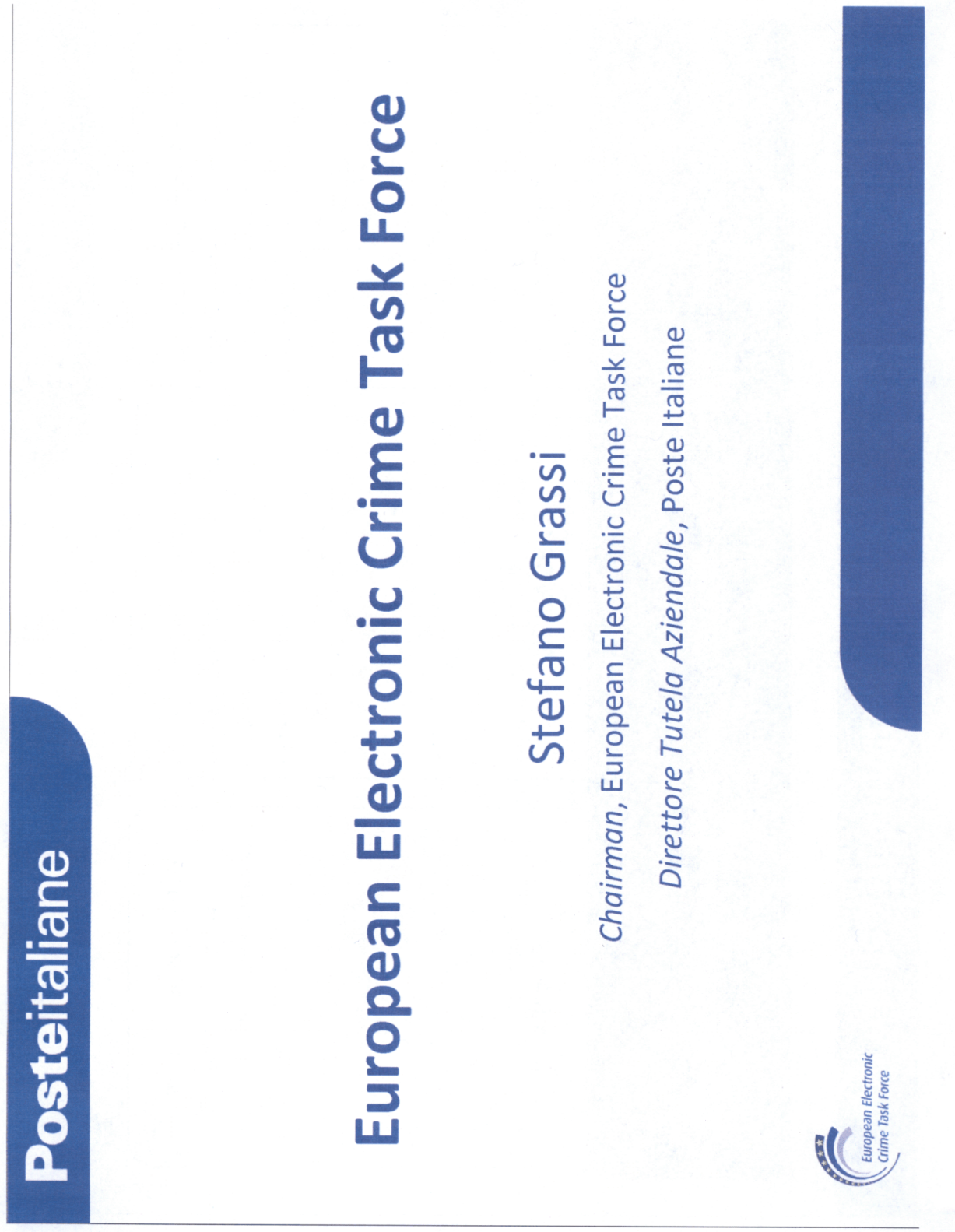
IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI ESTENSORE DEL PROCESSO VERBALE

DOTT. VALENTINO FRANCONI

Licenziato per la stampa il 20 febbraio 2013.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

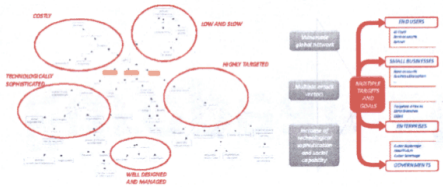
ALLEGATO 1


Posteitaliane
European Electronic Crime Task Force
Stefano Grassi
Chairman, European Electronic Crime Task Force
Direttore Tutela Aziendale, Poste Italiane
European Electronic Crime Task Force

Mission e Linee di Attività

Supportare l'analisi e lo sviluppo delle best practice di prevenzione, protezione e contrasto dei fenomeni di criminalità elettronica in Europa, attraverso la creazione di un'alleanza strategica tra organizzazioni private, pubbliche istituzioni, Forze dell'Ordine e enti di ricerca

ANALISI



- *Survey internazionali*
- *Sviluppo di demo e Proof of concept*
- *Progetti finanziati di Ricerca*
- *Linee guida per politiche sul cyber crime*

NETWORK

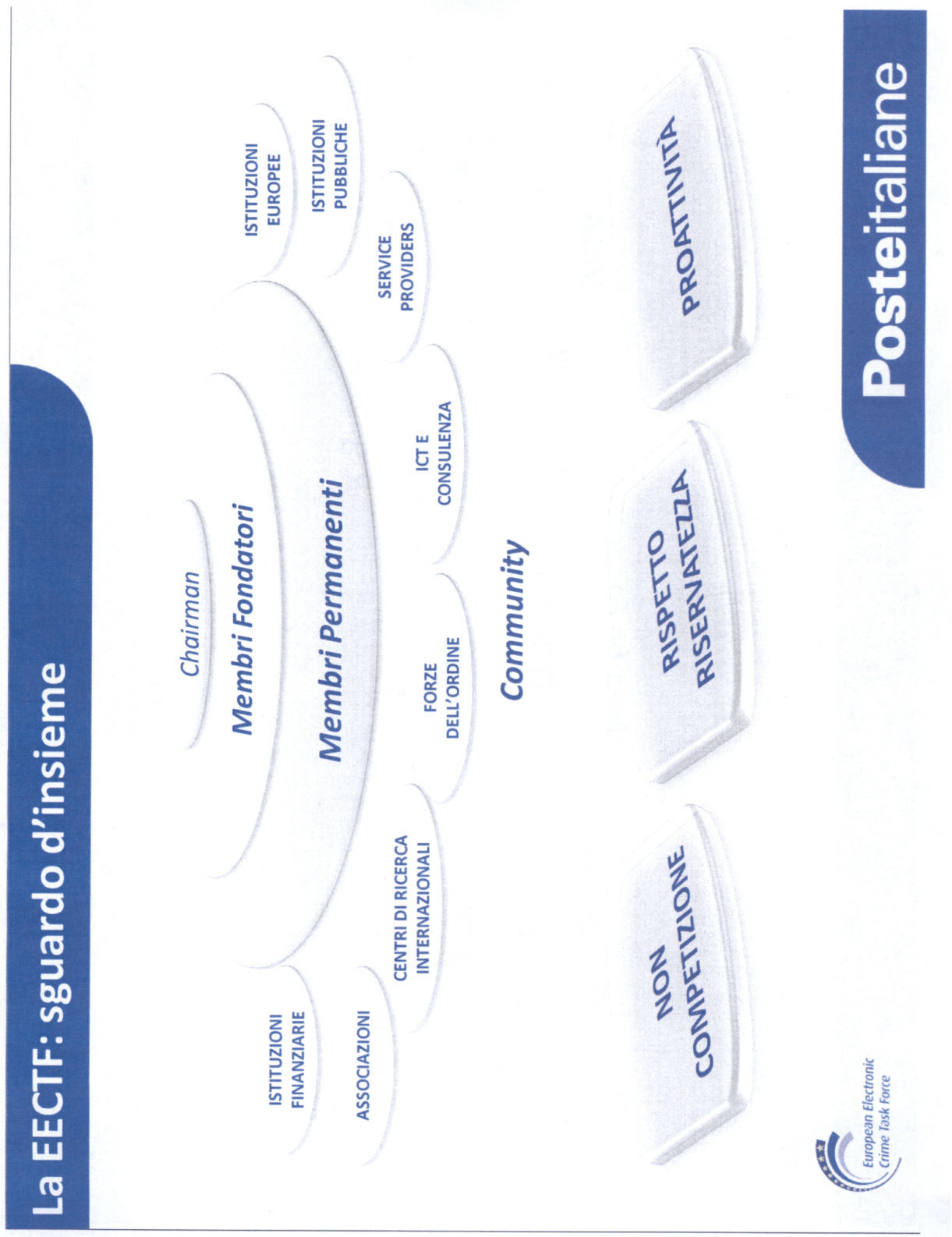
- *3 Membri Fondatori*
- *15 Membri Permanenti*
- *Più di 400 Membri della Community*
- *Cooperazioni Internazionali*

COMUNICAZIONE

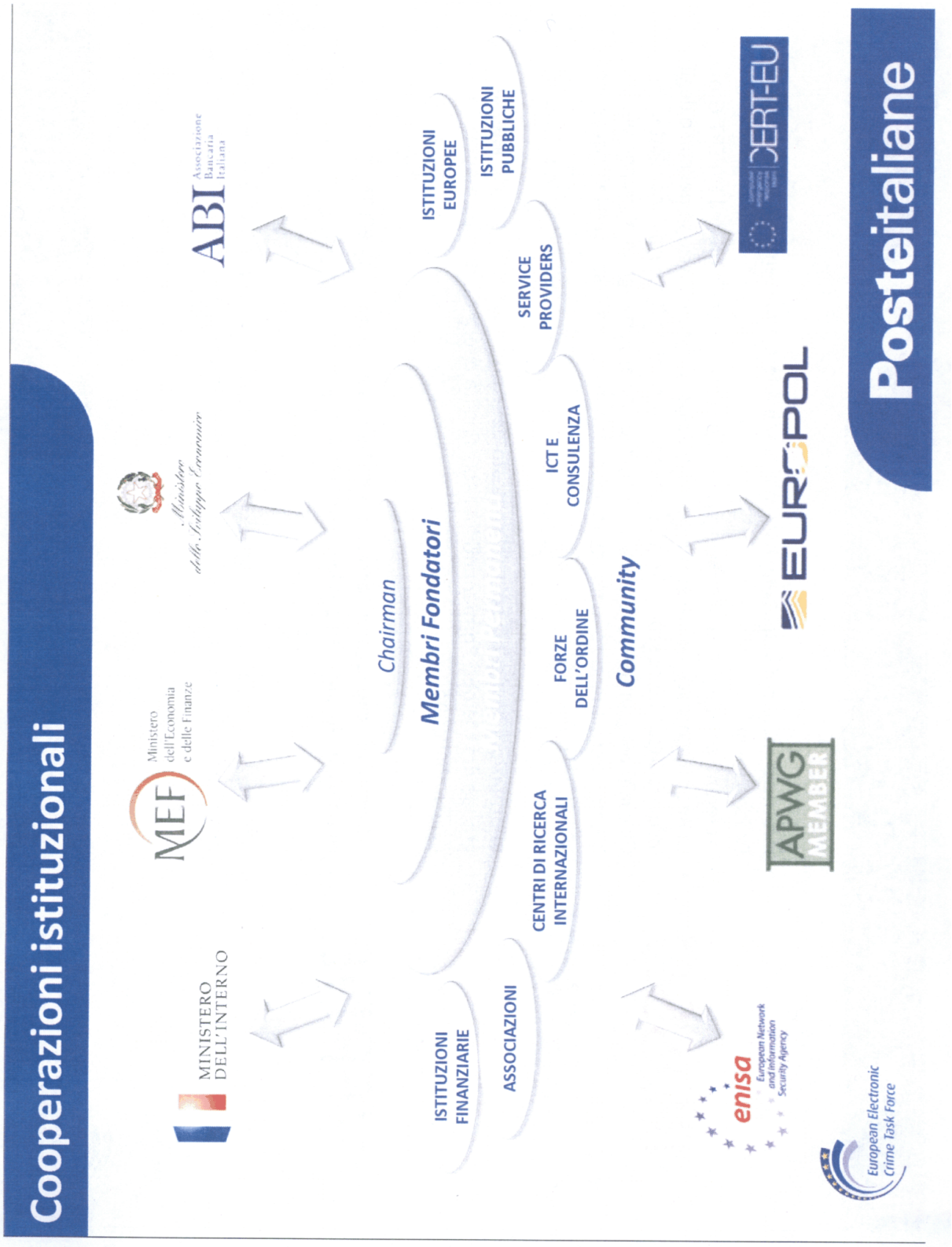
- *Newsletter Mensile*
- *Incontri Periodici dell'Expert Group*
- *3 Plenary Meeting per anno*
- *Iniziative di comunicazione congiunta*

European Electronic Crime Task Force

Posteitaliane


La EECTF: sguardo d'insieme
Chairman
Membri Fondatori
Membri Permanenti
ISTITUZIONI EUROPEE
ISTITUZIONI PUBBLICHE
SERVICE PROVIDERS
ICT E CONSULENZA
FORZE DELL'ORDINE
CENTRI DI RICERCA INTERNAZIONALI
ASSOCIAZIONI
ISTITUZIONI FINANZIARIE
Community
PROATTIVITÀ
RISPETTO RISERVATEZZA
NON COMPETIZIONE
Posteitaliane
European Electronic Crime Task Force


Membri Fondatori e Membri Permanenti
Posteitaliane
Chair
Membri Fondatori
United States Secret Service
polizia delle comunicazioni
GLOBAL CYBER SECURITY CENTER
unicri
TESORO
Romanian Police
Bulgarian Police
citibank
UniCredit
ca
RSA
The Security Division of EMC
SELEX ELSAG
KASPERSKY
Symantec
MasterCard Worldwide
VISA
AMERICAN EXPRESS
verizon
Membri Permanenti
Community
ISTITUZIONI EUROPEE
ISTITUZIONI PUBBLICHE
SERVICE PROVIDERS
ICT E CONSULENZA
FORZE DELL'ORDINE
CENTRI DI RICERCA INTERNAZIONALI
ASSOCIAZIONI
ISTITUZIONI FINANZIARIE
European Electronic Crime Task Force
Posteitaliane


Cooperazioni istituzionali
MINISTERO DELL'INTERNO
MEF
Ministero dell'Economia e delle Finanze
Ministero dello Sviluppo Economico
ABI
Associazione Bancaria Italiana
ISTITUZIONI FINANZIARIE
ASSOCIAZIONI
CENTRI DI RICERCA INTERNAZIONALI
FORZE DELL'ORDINE
ICT E CONSULENZA
SERVICE PROVIDERS
ISTITUZIONI EUROPEE
ISTITUZIONI PUBBLICHE
Chairman
Membri Fondatori
Community
enisa
European Network and Information Security Agency
European Electronic Crime Task Force
APWG MEMBER
EUROPOL
CERT-EU
Posteitaliane

Il codice di condivisione delle informazioni
ROSSO
• Informazioni non divulgabili e riservate ai soli referentipresenti agli incontri degli Expert Group.
• I referenti sono tenuti a non divulgare le informazioni al di fuori dell'EXPERT Group.
• Le informazioni scambiate in codice rosso possono essere discusse nel corso degli incontri dopo che ciascuno dei presenti abbia accettato il codice di condotta.
• Gli ospiti del gruppo (es. esperti esterni) che non appartengono al gruppo dei Membri Permanenti sono tenuti ad abbandonare la sala prima che tali discussioni abbiano inizio.
AMBRA
• Informazioni divulgabili solo nel contesto delle organizzazioni appartenenti al gruppo dei Membri Permanenti, per sole finalità operative di implementazione delle azioni opportune.
VERDE
• Informazioni che possono essere condivise con la Community EECTF, ma non ripubblicate in cartaceo o sul web (es. newsletter)
• Informazioni Pubbliche, divulgazione senza restrizioni di sorta, anche rispetto alla pubblicazione in cartaceo o sul web, sempre nel rispetto dei connessi diritti d'autore.
European Electronic Crime Task Force
Posteitaliane