

GIANCARLO MARCELLI

I REATI INFORMATICI A DANNO DELL'ISTITUTO NAZIONALE DELLA PREVIDENZA SOCIALE (I.N.P.S.)

SOMMARIO

1. Reati informatici e sistemi di sicurezza attuati dall'INPS. — 2. Tipologia e caratteristiche dei reati. — 3. Casistica. — 4. Allegato: sistemi di sicurezza e protezione del sistema informatico dell'INPS.

1. REATI INFORMATICI E SISTEMI DI SICUREZZA ATTUATI DALL'INPS.

L'Avvocatura dell'INPS, in occasione del IV Congresso Internazionale di informatica giuridica organizzato nel 1988 dal CED della Corte di Cassazione, concludeva la sua relazione in materia penale auspicando l'emanazione, da parte del legislatore, di un sistema compiuto di norme penali specifiche per i reati commessi a mezzo sistema informatico, rilevato e considerato che la diffusione dell'informatica nell'ambito della pubblica amministrazione aveva comportato dai primi anni 80 l'insorgere di forme di criminalità che attraverso programmi di superamento dei controlli inseriti nel sistema avevano cagionato rilevanti danni patrimoniali all'Ente.

Nel contempo rilevava la necessità di adottare sistemi di protezione adeguati agli attacchi, atti a garantire la sicurezza delle informazioni contro i pericoli di modifica, divulgazione, appropriazione e inserimenti illeciti, in considerazione della progressiva applicazione di procedure di elaborazione automatica dei dati a settori sempre più ampi di attività dell'Istituto e del sempre più esteso utilizzo del sistema che offre ad un numero crescente di operatori la possibilità di agire in maniera interattiva sui dati contenuti negli archivi e nei data-base, centrali e periferici.

Al riguardo va rilevato che l'INPS gestisce 40 milioni circa di soggetti tra assicurati, pensionati e altri che entrano in rapporto con l'Istituto. In particolare si tratta di 19 milioni di assicurati, pari all'85% della popolazione occupata, di 1.200.000 aziende e 14.200.000 pensionati, pari a circa l'80% delle pensioni erogate nel complesso.

* Il presente testo riproduce la relazione svolta al quinquennale Congresso sull'informatica giuridica organizzato dal CED-Cassazione e svoltosi a Roma dal 3 al 7 maggio 1993. Nel frattempo è stata approvata la l.

23 dicembre 1993, n. 547 (modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica), della quale si darà conto in un prossimo fascicolo.

L'importo complessivo netto pagato dall'INPS per le pensioni e le prestazioni temporanee rappresenta il 37% della spesa per protezione sociale, il 17% della spesa pubblica, il 9% del prodotto interno lordo.

Mediamente, ogni anno, l'Ente gestisce un volume di circa 144 milioni di documenti che entrano nel sistema per l'espletamento dell'attività produttiva, di cui 54 milioni per la gestione dell'area delle riscossioni e circa 90 milioni per l'emissione dei pagamenti delle prestazioni.

L'articolazione strutturale dell'Ente presenta una configurazione decentrata caratterizzata da circa 250 dipendenze periferiche.

Per lo svolgimento dei suoi innumerevoli compiti istituzionali in una struttura di tali dimensioni, l'Ente ha impostato una gestione informatizzata delle funzioni mediante un processo innovativo iniziato negli anni 70 con l'avvio dell'automazione, ossia l'acquisizione di dati attraverso operazioni di input da tastiera, che venivano prevalentemente affidate al servizio esterno per assenza di strutture interne idonee, come in tutte le Pubbliche Amministrazioni.

Negli anni 72-74 è stata impostata una forma di — acquisizione autonoma dei dati con l'introduzione del sistema di aggiornamento degli archivi con le tecniche batch e la consultazione degli archivi stessi in tempi reali.

Alla fine degli anni 70 è avvenuto il salto di qualità; la configurazione tecnologica dell'Ente si è andata modificando attraverso la distribuzione sul territorio della potenza di calcolo e dei volumi della memoria.

Rispetto a un sistema costituito da elaboratori centrali dedicati alle applicazioni dell'area delle prestazioni e dell'area della riscossione dei contributi, sono stati creati centri di elaborazione dati nelle Sedi periferiche, il che ha consentito la gestione di archivi locali con propria potenza di calcolo e l'aggiornamento in tempi reali sia degli archivi locali che di quello centrale, divenuto la grande base di dati storici e di sintesi delle informazioni provenienti dalla periferia, registra attraverso il Centro Elaborazione Dati dell'intero sistema informatico.

In sostanza è stato realizzato un disegno di decentramento capace di supportare il processo di conferimento alla periferia di autonomia decisionale e operativa.

Il sistema è tra i più complessi con un volume di due milioni di transazioni al giorno a livello regionale e con una potenzialità delle rete di comunicazione dati che si traduce in un volume medio orario di 700 milioni di bytes.

Un sistema di tali dimensioni e così articolato, con assegnazione di responsabilità sempre maggiori agli operatori, talvolta unici, non poteva essere immune da attacchi, che sono puntualmente avvenuti ad opera di dipendenti infedeli addetti alla procedura, a cominciare dai primi anni 80, prima a livello centrale e successivamente a livello periferico, quando quest'ultimo ha assunto autonomia decisionale e operativa.

L'INPS, per realizzare un sistema di sicurezza logica dei dati e delle informazioni, con disposizioni impartite nel tempo ha individuato e posto in essere vari accorgimenti, mediante interventi sia sul piano amministrativo, con circolari ed ordini di servizio, che sul piano tecnico, finalizzati alla garanzia, alla integrità e alla riservatezza del sistema e dei dati; se ne elencano alcuni:

— identificazione di ogni operatore addetto al sistema attraverso lettori di tessere magnetiche « badge » collegati a tutti i terminali e da codici « password » che il sistema richiede prima di iniziare l'elaborazione;

— sostituzione delle parole chiave con frequenza almeno mensile ed anche più frequentemente secondo le contingenze e sempre in caso di trasferimento dell'operatore ad altro reparto;

— particolari accorgimenti e sorveglianza, anche con guardie giurate, in determinati orari e circostanze, alle porte di accesso alla sala computers con nomina di un responsabile;

— obbligo per gli operatori di annotare su registro: orario di utilizzo, procedure attivate, nome, cognome e firma;

— controlli amministrativi sistematici di qualità con una campionatura non inferiore al 10% su tutto l'iter delle pratiche a qualsiasi titolo definite e controllo generalizzato e non a campione per alcune procedure a maggior rischio con soglia di sicurezza fissata in L. 200.000 per i saldi passivi delle denunce nominative mensili;

— compilazione di verbali da consegnare dagli operatori mensilmente al Responsabile del controllo sull'attività produttiva e sicurezza dati.

Per una più dettagliata conoscenza delle tutele adottate si rinvia al documento allegato.

I correttivi posti alla sicurezza del sistema ed controlli sull'attività degli operatori, se hanno permesso il raggiungimento di una sufficiente tutela delle procedure, non sembrano tuttavia avere raggiunto la sicurezza assoluta se è vero che le aggressioni sono continuate e ciò sia perché la protezione degli archivi ad accesso diretto e dei data-base, consultabili e modificabili in maniera interattiva da terminale, presenta un elevato grado di complessità, sia perché i controlli diretti a prevenire accessi ed interventi non autorizzati hanno dovuto conciliare l'esigenza di cautela dai rischi con l'esigenza di non ridurre la funzionalità del sistema e il risultato del prodotto sia perché l'istituzione dell'operatore unico, se da un lato è risultata ampiamente positiva sotto il profilo organizzativo e produttivo, dall'altro ha aumentato la possibilità di effettuare azioni truffaldine fidando nella fiducia accordata. Si può convenire con l'orientamento generale secondo il quale, nell'impossibilità di raggiungere una sicurezza totale e assoluta, che comunque andrebbe a danno del risultato, va fatta opera soprattutto di prevenzione.

Un osservatorio permanente sui procedimenti penali incardinati per reati commessi a danno dell'ente o comunque interessanti l'INPS, è costituito presso l'Avvocatura Centrale, che acquisisce notizie, per la sua funzione istituzionale di coordinamento, dagli Uffici Legali presenti in tutte le Sedi e attraverso il collegamento con gli archivi della Suprema Corte di Cassazione (ITALGIURE).

All'Avvocatura Centrale — integrata per la sua attività nella rete informatica dell'Istituto, così come avviene per tutti gli uffici legali — affluiscono inoltre, per le specifiche competenze, le relazioni ispettive redatte in seguito ad accertamenti dall'Ispettorato Centrale e copia di tutte le denunce presentate all'A.G. dal Direttore Generale e dai Direttori delle Sedi, al fine di poter seguire i procedimenti sin dalla fase delle indagini preliminari e provvedere alla successiva costituzione di parte civile ogni volta che sia derivato danno di qualsiasi natura.

Un'azione importante per la comprensione dei meccanismi di attacco e per i successivi interventi da parte delle Direzioni competenti per la predisposizione dei sistemi di difesa viene svolta dall'Ispettorato Centrale dell'Istituto, il quale fornisce la massima collaborazione, oltre che all'Avvocatura, alla Magistratura ai fini di giustizia.

2. TIPOLOGIA E CARATTERISTICHE DEI REATI.

I reati informatici a danno dell'Istituto, dei quali si ha conoscenza, sono stati commessi quasi esclusivamente all'interno dell'ente e prevalentemente ad opera di dipendenti infedeli addetti al sistema, mediante interventi sulla procedura per la liquidazione di prestazioni e per l'accreditamento dei contributi alle aziende. Trattasi di operatori che talvolta hanno eluso i sistemi di sicurezza aggirandoli e talvolta hanno agito sui programmi di modifica e correzione.

In un caso è avvenuto furto di programmi e archivio dati.

L'attacco è stato portato anche ad opera di aziende mediante consegna all'INPS di documenti magnetici contenenti dati falsi relativi alla retribuzione e alla contribuzione dei lavoratori dipendenti occupati.

Non si è a conoscenza di intromissioni nella banca dati dall'esterno e comunque non esistono procedimenti penali per tali fattispecie.

Sono stati chiamati a rispondere in correttezza con i pubblici dipendenti i beneficiari delle prestazioni non dovute, consulenti di lavoro ed anche dipendenti di patronato.

Il danno patrimoniale arrecato all'ente dalle azioni criminose scoperte è stato attenuato dalle restituzioni spontanee e coattive avvenute ad opera dei beneficiari di prestazioni non dovute e dai risultati delle azioni civili di recupero sul patrimonio e sul trattamento di fine rapporto dei dipendenti condannati e destituiti.

Il danno, in termini relativi e complessivi, considerati la dimensione del sistema, il numero delle transazioni e la quantità di denaro in circolazione, non può ritenersi elevato ed anche il numero dei dipendenti tratti a giudizio, in relazione al numero degli addetti, appare esiguo.

Non va sottaciuto che se il danno immediato può essere non rilevante, lo stesso diventa consistente nel lungo termine. Basti pensare all'inserimento di contributi finalizzati alla concessione di pensioni non dovute o ad aumenti delle stesse. Ove l'azione criminosa non venisse scoperta il danno, in tali casi, può protrarsi per tutta la durata della vita del falso pensionato ed oltre, quindi anche per decine di anni.

Va pure posto in evidenza che, a differenza di quanto può accadere presso banche ed enti privati, tutti i fatti scoperti sono stati denunciati con immediatezza ai sensi dell'art. 331 cod. proc. pen. e ciò sia per il preciso obbligo sanzionato dall'art. 361 cod. pen., sia per i principi di trasparenza ai quali si ispira l'Istituto.

Molti casi sono stati scoperti nella prima fase della condotta, il che ha impedito di portare il crimine ad ulteriori conseguenze con incremento del danno.

Alle azioni dell'Istituto si sono aggiunti i giudizi di responsabilità amministrativa promossi dalla Procura Generale della Corte dei Conti per il danno all'Eraio.

Si è potuto osservare che gli imputati di reati commessi dopo l'entrata in vigore del nuovo codice di procedura penale in prevalenza non hanno affrontato il dibattimento, ma hanno chiesto e ottenuto l'applicazione della pena su richiesta, secondo il dettato dell'art. 444 cod. proc. pen., sia in sede di udienza preliminare che dibattimentale e che talvolta l'accoglimento è stato subordinato dal giudice al ristoro delle pretese risarcitorie dell'Istituto.

I *computer crimes* sono stati in prevalenza commessi al Centro-Nord del paese.

È emerso altresì che il dipendente infedele è prevalentemente di età media, con una notevole preparazione tecnica, stimato sul posto del lavoro e nella società, immune da precedenti penali e disciplinari e che le giustificazioni addotte sono state: necessità di denaro, convinzione di avere diritto ad una retribuzione superiore ad altri dipendenti di pari qualifica in relazione all'attività svolta, sfida al sistema, certezza dell'impunità ed anche la convinzione che, se scoperti, la pena non sarebbe stata severa, considerato che il fatto non era previsto come reato nel codice.

La scoperta dei fatti criminosi è avvenuta in seguito a controlli interni, ad interventi di colleghi di ufficio, a segnalazioni anonime, ad errori commessi dagli autori e per mero caso.

È da ritenere fondata l'ipotesi, accennata in qualche atto processuale, che non tutti gli autori delle azioni criminosi siano stati scoperti e che dei complici annidati all'interno dell'ente abbiano partecipato, rimanendo nell'ombra, ad alcune delle complesse fasi propedeutiche al risultato delle azioni medesime.

Alla difesa dagli attacchi portati dall'esterno ad opera di aziende che forniscono falsi dati relativi a contributi possono dare un grande contributo i collegamenti già realizzati con il Fisco, le Camere di Commercio, l'Anagrafe dei Comuni.

I campi di intervento degli autori dei computer crimes spaziano in molte delle materie trattate dall'Istituto: dalle posizioni contributive alle pensioni d'invalidità, di vecchiaia, di anzianità, alle ricostituzioni, alle prestazioni minori, alle indennità di disoccupazione e di malattia.

Gli incassi degli assegni e delle cedole emessi dopo le manipolazioni sono avvenuti sia presso gli uffici postali che presso le banche: si condividono i dubbi espressi in alcune sentenze circa la facilità con cui è stato possibile negoziare assegni non trasferibili intestati a terzi.

I reati contestati agli autori delle azioni criminosi sono stati la truffa aggravata, la falsità materiale e ideologica in atti pubblici ed anche il peculato, l'abuso d'ufficio, la rivelazione di segreti di ufficio, la corruzione in atti di ufficio, la soppressione di documenti e, in un caso, l'associazione per delinquere.

Per la contestazione dei reati, l'uso necessitato delle norme previste dal codice penale attuale è avvenuto in maniera disforme e applicando norme diverse per casi analoghi, avvertendosi chiaramente che la qualificazione giuridica dei fatti e le sentenze risentono della diversa sensibilità giuridico-informatica dei magistrati.

Nelle sentenze citate, tranne una, non vi è stato un sufficiente approfondimento sulla natura del reato informatico, del documento, del falso specifico, né pare possa essere di giustificazione la mancanza di una norma specifica di riferimento.

Vanno segnalate in tema di peculato, la decisione della Suprema Corte di Cassazione relativa alla fattispecie di cui al n. 1 della casistica e, circa il valore probatorio dei tabulati, come rappresentazione fedele dei dati immessi nel calcolatore elettronico, la fattispecie di cui al caso n. 2.

Resta l'esigenza, ormai indifferibile, di una normativa sui *computer crimes* che preveda come reato nuove figure di illeciti in materia informatica per i quali la coscienza sociale reclama una tutela penalistica.

3. CASISTICA.

La presente casistica comprende la quasi totalità dei procedimenti penali per reati commessi a danno dell'INPS, dei quali si è venuti a conoscenza, dall'inizio degli anni 80 ad oggi.

Di questi soltanto i primi tre sono pervenuti all'esame della Corte Suprema di Cassazione.

L'elenco è in ordine cronologico e l'Avvocatura ha rappresentato e difeso gli interessi dell'Istituto mediante costituzione di parte civile in tutti i processi.

Caso n. 1.

Fatto: un dipendente dell'ente, addetto all'ufficio pensioni e successivamente al centro elettronico, interveniva sull'archivio informatico duplicando ordinativi di pagamenti già liquidati ai titolari effettivi, che poi incassava personalmente mediante false deleghe presso vari uffici postali.

Le indagini ed il procedimento penale *de quo* hanno avuto origine dalla denuncia di un assicurato, il quale era andato a chiedere chiarimenti all'INPS circa un sovrappiù figurante a titolo di reddito sul proprio modello 101, somma in più che egli non aveva mai ricevuto.

Il caso, scoperto nel 1983 e non ripetibile negli stessi termini in virtù degli accorgimenti tecnici e delle modifiche amministrative apportate successivamente ai fatti, merita attenzione per la qualificazione giuridica data ai fatti.

Imputazione: il dipendente è stato tratto a giudizio per rispondere dei reati di peculato e falsità ideologica in atti pubblici (artt. 314-479 cod. pen.).

Esito: il Tribunale ha dichiarato l'imputato responsabile dei reati ascrittigli, modificando però la imputazione di peculato in quella di truffa aggravata.

La sentenza è stata impugnata dall'imputato, dalla Procura Generale e dall'INPS, parte offesa.

La Corte d'Appello, in parziale riforma, ha dichiarato l'imputato colpevole del reato di peculato continuato e di truffa aggravata, in accoglimento della tesi del Procuratore Generale e confermando nel resto.

Motiva la sentenza della Corte: «l'imputato, mediante la formazione *ex novo* di ordinativi di pagamento formalmente validi ma sostanzialmente falsi, compiva atti di disposizione di denaro pubblico e ne conseguiva, fin *ab initio*, la disponibilità giuridica, anche se per la materiale appropriazione occorreva ancora la falsificazione della delega ed il concorso inconsapevole dell'ufficiale postale che effettuava il pagamento. Pertanto l'ipotesi in oggetto deve giuridicamente qualificarsi come peculato per appropriazione».

La Corte di Cassazione, Sezione VI Penale, con sentenza n. 693 del 6 marzo 1989, ha rigettato il ricorso proposto dall'imputato, così motivando: «la Corte di Appello ha fatto corretta applicazione del principio per il quale in tema di peculato la nozione di possesso va intesa in senso ampio, come rapporto di fatto dell'agente con il denaro oggetto dell'appropriazione, non rilevando neppure che esso sia detenuto da altri quando l'agente ne abbia la disponibilità giuridica, cioè possa — mediante un atto dispositivo di sua competenza — conseguirne la materiale detenzione».

Caso n. 2.

Fatto: Un dipendente mediante uso dell'elaboratore elettronico accreditava versamenti contributivi non effettuati in favore di aziende.

I fatti erano stati scoperti in seguito a controlli interni, disposti dopo una segnalazione anonima pervenuta all'INPS, che avevano appurato come la frode si fosse sviluppata su due direttrici: 1) falsificazione materiale dei modelli con cui il datore di lavoro denuncia mensilmente l'importo dei contributi per i lavoratori dipendenti (modelli DM 10/M); 2) immissione di dati falsi nel calcolatore dell'ente.

I DM 10/M pagati venivano rimessi giornalmente dalle banche alla sede INPS, la quale li riepilogava in modelli, li contabilizzava e quindi li inseriva nell'elaboratore per l'aggiornamento dell'archivio. L'attività di falsificazione si è concretizzata, nei confronti dell'INPS, nella immissione nel calcolatore di dati falsi, attestanti sostanzialmente che una ditta aveva presentato modelli con saldo pagato, mentre in realtà ciò non corrispondeva al vero. Nei confronti del privato interessato alla frode, la falsificazione si è concretizzata nella apposizione sulle copie dei DM 10/M di un falso timbro di banca a quietanza per cui in tal modo il privato era in condizione di dimostrare, ad un eventuale controllo, di avere corrisposto all'INPS i contributi dovuti.

In sostanza, la falsificazione riguardava gli atti minimi essenziali per provare il pagamento: il DM 10/M quietanzato per il privato e la memoria magnetica del calcolatore; quest'ultima falsificazione, agendo direttamente sull'elaboratore, saltava tutta la procedura di acquisizione contabile dei dati con i relativi riscontri.

Imputazione: *a*) falsità materiale in atti pubblici (art. 476 cod. pen.) per avere apposto falsi timbri di banche sui moduli per il versamento dei contributi; *b*) truffa aggravata (art. 640 cpv. n. 1) per avere inserito nel cervello elettronico INPS dati non veritieri circa il pagamento dei contributi da parte di una ditta.

Esito: con sentenza del 20/6/85, il Tribunale di Roma, Sez. VI Penale, ha dichiarato l'imputato colpevole dei reati ascrittigli.

La Corte di Appello ha dichiarato estinti i reati per prescrizione.

La Corte di Cassazione ha rigettato il ricorso proposto dall'imputato che chiedeva l'assoluzione dichiarando che sussiste la prova della sua responsabilità.

Osservazioni: La sentenza del Tribunale, oltre a fornire un notevole contributo all'analisi della criminalità informatica, ha affermato che sul piano giuridico i tabulati prodotti dall'INPS sono documenti formali da considerare atti pubblici in quanto documenti probatori della avvenuta falsificazione, che la loro provenienza dal calcolatore, quali elaborati dei dati memorizzati, è attestata dall'ente che li ha rimessi e che il loro valore probatorio è quindi nella rappresentazione fedele dei dati immessi nel calcolatore.

Anche sotto il profilo della frode, la decisione aggiunge alla tradizionale indicazione della falsificazione del documento cartaceo quello della immissione dei dati falsi nel calcolatore, attribuendo un'autonoma rilevanza giuridica, come elemento costitutivo del reato di truffa, alla manipolazione informatica.

Caso n. 3.

Fatto: un dipendente rilevava dall'archivio cartaceo le domande di pensioni respinte, alterava il referto medico, modificava i ricorsi respinti come accolti, contraffaceva sui prospetti di liquidazione la firma del

Capo Reparto, quindi modificava i dati autentici relativi alle pratiche respinte contenute nell'elaboratore elettronico conformemente alle falsificazioni documentali già operate: procedimento, quest'ultimo, indispensabile ai fini dell'erogazione del trattamento pensionistico in quanto la stampa del libretto di pensione e degli elenchi del mandato di pagamento è effettuata esclusivamente dal centro elettronico.

Il dipendente operava tale falsificazione ovviamente allo scopo di perseguire una utilità in denaro.

L'indagine amministrativa e la successiva denuncia alla A.G. erano scaturite a seguito del ritrovamento presso l'ufficio di due pratiche con documenti visibilmente falsificati.

I fatti sono avvenuti nel 1984; sono stati individuati e tratti a giudizio con il dipendente i 22 beneficiati dall'azione criminosa.

Imputazione: truffa aggravata, falsità materiale in atti d'ufficio, corruzione per atti contrari ai doveri d'ufficio (artt. 640 comma 2, n. 1 - 476 - 319 cod. pen.).

Esito: con sentenza dell'11 ottobre 1986 il Tribunale di Roma, Sez. II Penale ha dichiarato il dipendente colpevole dei reati ascrittigli, modificando l'imputazione di corruzione in quella di interesse privato in atti d'ufficio e condannandolo alla pena di anni 4 e mesi 6 nonché all'interdizione dai pubblici uffici per anni 5.

Il Tribunale ha motivato affermando che il procedimento amministrativo ha natura documentale e che qualunque alterazione dello stesso non può realizzarsi se non attraverso un falso in atti pubblici.

La Corte d'Appello di Roma, Sez. II Penale, con decisione n. 4117/89 ha confermato l'impugnata sentenza nei confronti del dipendente.

La Corte di Cassazione Sez. V Penale con sentenza n. 1094 del 19 dicembre 1991 ha dichiarato l'estinzione dei reati per prescrizione.

Danno: rilevante; sono in corso le azioni di recupero.

Caso n. 4.

Fatto: Due individui, forniti di falsi documenti di identità, si presentarono nel 1983 presso lo sportello di un ufficio postale per riscuotere delle pensioni; furono arrestati in flagranza essendo in corso indagini su una truffa a danno dell'INPS commessa da un dipendente il quale, al momento del rinnovo — tramite il sistema elettronico — degli ordini di pagamento delle pensioni, stampava due esemplari di ognuno; il doppio veniva inviato ad un ufficio postale, diverso da quello di localizzazione della pensione regolare, dove il dipendente o i suoi complici, a seconda dei casi, si recavano per l'incasso forniti di false deleghe e falsi libretti di pensioni.

Imputazione: Truffa aggravata e continuata in concorso, falsità materiale in atti pubblici (artt. 640, comma 2, n. 1 - 476 cod. pen.).

Esito: con sentenza del 17 gennaio 1992 il Tribunale di Roma, sez. XI Penale, decidendo con rito abbreviato, ha dichiarato l'imputato colpevole dei reati ascrittigli condannandolo alla pena di anni 3 e L. 1.000.000 di multa.

La sentenza è stata appellata.

Danno: Rilevante, in fase di recupero.

Caso n. 5.

Fatto: un dipendente addetto alla procedura informatica interveniva sul sistema in modo da liquidare somme di denaro a titolo di indennità di di-

soccupazione in agricoltura in favore di soggetti non aventi diritto ai quali faceva pervenire assegni.

La somma incassata veniva divisa con l'autore dell'azione criminosa, il quale distruggeva le matrici degli assegni non esistendo una pratica sottostante.

I mandati di liquidazione venivano sottoposti alla firma dei superiori mescolati a numerosi altri regolari.

I fatti sono stati scoperti dall'Istituto durante una verifica sulla posizione contributiva di una assicurata la quale aveva chiesto la prosecuzione volontaria dei contributi.

La denuncia all'A.G. è stata immediata.

Imputazione: a) falsità materiale in atti pubblici (art. 476, comma 1 cod. pen.) per avere, agendo in accordo con i singoli beneficiari, inserito nel terminale piccole difformità nei dati e nelle generalità dei beneficiari, relativamente alla data, al luogo di nascita e al sesso, allo scopo di formare assegni a loro favore, senza che nessuno di essi ne avesse diritto; b) truffa aggravata (art. 640 comma 2 n. 1 cod. pen.) per avere, mediante artifici e raggiri, costituiti nel sottoporre alla firma del Dirigente di sede e di quello di reparto i modelli IP/6 *bis* che riportavano accanto a soggetti aventi diritto anche i nominativi di soggetti che non avevano diritto a prestazione alcuna, indotto in errore l'INPS che ordinava effettuazione di pagamenti a favore di tali persone.

Danno: non è stato rilevante e in gran parte sono state recuperate le somme erogate.

Esito: tutti gli imputati hanno chiesto e ottenuto il patteggiamento di cui all'art. 444 cod. proc. pen.

Caso n. 6.

Fatto: un dipendente addetto al settore liquidazione indennità di malattia predisponendo modelli per liquidazione di somme in favore di assicurati per importi superiori a quelli dovuti, poi inseriva i dati nel sistema informatico, cui seguiva la stampa automatica degli assegni, che venivano ritirati personalmente dallo stesso e recapitati ai beneficiari, suoi conoscenti, i quali li versavano sui propri conti correnti o li giravano al dipendente, ripartendosi il ricavato.

Venivano tratti a giudizio l'impiegato e gli indebiti beneficiari.

Imputazione: peculato (art. 314 cod. pen.) perché, nella qualità di impiegato pubblico, inseriva nel terminale nominativi ottenendo così la stampa di assegni per vari importi relativi a presunte liquidazioni di indennità comunque non dovute, impossessandosi delle somme corrispondenti.

L'azione criminosa veniva scoperta nel 1989 da un collega di stanza, il quale ne dava notizia al capo Reparto; seguiva l'immediata denuncia all'A.G.

Danno: è stata recuperata in parte la somma e sono in corso le azioni di recupero nei confronti di tutti i correi.

Esito: tutti gli imputati hanno chiesto e ottenuto il patteggiamento di cui all'art. 444 cod. proc. pen.

Caso n. 7.

Fatto: Un dipendente operatore unico addetto al ricalcolo delle pensioni, usando l'elaboratore informatico, utilizzava l'importo in più che

avrebbe dovuto essere reintroitato dall'INPS per creare una nuova pratica a favore di nomi di fantasia o di persone realmente esistenti, ma non risultanti sull'archivio pensioni, ottenendo la stampa degli assegni relativi e delle cedole di riscontro; dopo di che falsificava i modelli riepilogativi in modo tale che il totale complessivo fosse uguale al totale delle cedole di riscontro cui si riferivano quei moduli, rendendo vana ogni possibilità di scoprire l'illecito mediante controllo cartaceo.

Inoltre l'autore non inviava all'elaboratore centrale dell'INPS le posizioni falsamente create per cui nelle memorie elettroniche dell'Istituto non rimaneva traccia delle fraudolente operazioni effettuate, per cui anche ogni controllo su base informatica avrebbe dato esito negativo.

Gli assegni venivano incassati presso varie banche direttamente dall'autore e dagli indebiti beneficiari, con i quali venivano ripartiti a metà gli importi.

L'azione criminosa, attuata per molti anni, è stata scoperta in occasione di una verifica interna sui modelli di reincasso e immediatamente denunciata all'A.G.

Sono stati rinviati a giudizio tutti i beneficiati degli assegni.

Imputazione: *a)* peculato (art. 314 cod. pen.) per essersi appropriato di assegni dei quali aveva il possesso per ragione del suo servizio di addetto al sistema elettro-contabile, assegni che materialmente compilava, parte dei quali intestati a persone non aventi diritto e che incassava; *b)* falsità materiale in atti pubblici (artt. 476 cod. pen.) per avere formato numerosi ordinativi di spesa in favore di persone non aventi diritto.

Esito: gli imputati hanno richiesto e ottenuto il patteggiamento di cui all'art. 444 cod. proc. pen.

Danno: rilevante. È in corso l'azione di recupero verso beneficiari e sui beni immobili del dipendente destituito.

Caso n. 8.

Fatto: un dipendente addetto all'ufficio riscossione contributi, acquisiva nell'archivio elettronico versamenti di contributi in favore di aziende che nulla avevano versato, in accordo con un consulente, il quale creava false ricevute, (modelli DM 10/M) con falsi timbri di banche, per tacitare i clienti che gli avevano consegnato denaro per effettuare il pagamento dei contributi all'INPS.

Reati contestati: *a)* falsità materiale in atti pubblici (art. 476 cod. pen.) per avere, al fine di commettere in concorso più delitti di truffa aggravata e di appropriazione indebita, falsificato le posizioni contributive di più aziende, creando falsi modelli DM 10/M e dolosamente intervenendo sugli archivi meccanografici ed elettronici dell'INPS facendo risultare registrazioni non veritiere di pagamenti dei contribuenti in verità non versate e facendo poi sparire sia le contabili riepilogative che le attestazioni di versamento corrispondenti ad altre ditte che in realtà avevano regolarmente versato i contributi; *b)* del delitto di abuso d'ufficio (art. 323, comma 2, cod. pen.) per avere in concorso abusato del proprio ufficio allo scopo di procurarsi un ingiusto vantaggio patrimoniale.

I fatti sono stati scoperti dall'INPS nel 1990, in seguito a controlli sulle posizioni contributive delle aziende ed immediatamente denunciati all'A.G.

Esito: è stata tenuta l'udienza preliminare e pronunciato decreto che dispone il giudizio.

Danno: l'Istituto ha già recuperato parte delle somme mediante versamenti effettuati dal consulente e dalle aziende truffate.

Caso n. 9.

Fatto: un dipendente, operatore unico addetto all'archivio informatico delle posizioni assicurative dei lavoratori dipendenti, accreditava contributi in favore di non aventi diritto, simulando l'esistenza di modelli d'uso dei datori di lavoro normalmente destinati alle regolarizzazioni contributive.

Con tale azione le false contribuzioni acquisite nell'archivio sono state fatte figurare come riferite a datori di lavoro effettivamente esistenti ed iscritti all'INPS, le cui matricole aziendali sono apparse formalmente coerenti sugli estratti conto. Le acquisizioni in archivio sono prive dei supporti cartacei.

La truffa ha consentito la liquidazione della pensione di vecchiaia, il perfezionamento del diritto alla pensione di anzianità e l'anticipazione dell'età pensionabile, in virtù della contribuzione aggiuntiva, in favore di soggetti con contribuzione mancante o insufficiente ed anche in favore di residenti in sedi diverse.

Imputazione: abuso d'ufficio, truffa aggravata e corruzione per atto contrario ai doveri d'ufficio (artt. 323 - 640 cpv. - 319 cod. pen.).

La truffa è stata scoperta dall'ente in fase di liquidazione delle pensioni e la denuncia all'A.G. è stata immediata.

Danno: l'accertamento è in corso, mediante verifica di tutte le posizioni, da parte dell'Ispettorato, il quale ha ricostruito tutte le fasi ed i meccanismi dell'azione criminosa.

Sono in corso le azioni di recupero.

Esito: è stata fissata l'udienza preliminare.

Caso n. 10.

Fatto: l'operatore unico di una sede, che godeva di grande stima ed affidamento, agendo sulla procedura automatizzata, ha creato in archivio una posizione assicurativa in favore di una sola persona che non aveva mai avuto contribuzione in quella gestione, facendole così pervenire assegni per disoccupazione agricola ed assegni familiari.

La scoperta del fatto è avvenuta a seguito di segnalazione anonima pervenuta all'INPS e dopo i primi accertamenti la denuncia è stata presentata alla locale Procura della Repubblica.

Imputazione: abuso d'ufficio e falsità ideologica in atti pubblici (artt. 323 e 476 cod. pen.).

Esito: l'imputato ha patteggiato la pena, ai sensi dell'art. 444 cod. proc. pen., in sede di udienza preliminare.

Danno: la somma è stata interamente restituita, gravata di interessi e rivalutazione, prima del patteggiamento, su richiesta del giudice per le indagini preliminari.

Caso n. 11.

Fatto: un dipendente addetto alla gestione delle posizioni assicurative, con accesso agli archivi del sistema informatico, accreditava contributi non versati in favore di non aventi diritto al fine di fare ottenere tratta-

menti pensionistici e arretrati di importo consistente. L'azione criminosa è stata posta in essere in accordo con un funzionario di patronato. Entrambi si impossessavano delle somme loro consegnate dai beneficiati a titolo di versamenti volontari o per riscatto di periodi contributivi scoperti e ad altro titolo. La documentazione cartacea predisposta veniva distrutta dopo l'inserimento dei dati nell'archivio informatico. Numerose pensioni sono state liquidate in favore di non aventi diritto.

I fatti sono stati scoperti dall'Istituto in fase di revisione di alcune posizioni ed immediatamente denunciati all'A.G.

Imputazione: falsità materiale e ideologica in atti pubblici, truffa aggravata e continuata, associazione per delinquere, corruzione per atto contrario ai doveri d'ufficio, soppressione di documenti (artt. 476 - 479 - 640 n. 1 e 2 416 - 319 - 490 cod. pen.).

Danno: consistente; le somme sono state in parte restituite dai singoli beneficiati e in parte recuperate. Sono in corso le azioni di recupero per il residuo.

Esito: molti degli imputati hanno patteggiato la pena. Il dipendente è stato dichiarato penalmente responsabile e condannato in primo grado alla pena di anni 5 di reclusione, all'interdizione perpetua dai pubblici uffici ed al risarcimento del danno in solido con i beneficiati di somme non dovute. La decisione è stata appellata.

Caso n. 12.

Fatto: nel corso di una complessa inchiesta giudiziaria nei confronti di una società per evasione fiscale, corruzione ed altro è emerso che la medesima truffava l'INPS mediante presentazioni di falsi dati contributivi elaborati elettronicamente in maniera da indurre in errore l'INPS.

La truffa era finalizzata al pagamento di contributi inferiori al dovuto ed era così articolata: l'azienda consegnava ai lavoratori il modello riepilogativo dei salari corrisposti (mod. 01/M) esattamente corrispondente all'importo delle buste-paga e del modello 101. All'INPS invece veniva consegnato un mod. 01/M con importi inferiori, ma corrispondente esattamente ai modelli (DM 10/M) contenenti le retribuzioni, anch'essi di importo inferiore al corrisposto.

I fatti sono stati scoperti nel 1989.

Imputazione: truffa aggravata e continuata (artt. 81, 110, 61 n. 7, 640 cpv. n. 1 cod. pen.) perché, quali amministratori, soci, dirigenti e consulenti della società in concorso tra loro e con altre persone soggette alla loro autorità e direzione, inducevano in errore l'INPS con l'artificio di ridurre del 40% l'imponibile contributivo sul supporto magnetico elaborato dal C.E.D. della società contenente i dati relativi ai dipendenti, così procurandosi un ingiusto profitto con corrispondente danno per l'Ente.

Danno: rilevante. Sono in corso le azioni per il recupero.

Stato: in attesa della fissazione del dibattimento.

Caso n. 13.

Fatto: un dipendente addetto alla gestione, mediante la procedura informatica, delle posizioni assicurative, cedeva ad un'agenzia privata di assistenza pensionistica di cui era cotitolare la moglie, i programmi di gestione in dotazione all'INPS.

L'azione criminosa è stata scoperta nel 1991 in seguito ad accertamenti sull'attività dell'azienda e denunciata dall'Istituto all'A.G.

Imputazione: rivelazione di segreti d'ufficio (art. 326 cod. pen.) per avere rivelato ed agevolato la conoscenza di documenti di proprietà dell'Ente pubblico riguardante: a) il programma di gestione degli archivi delle posizioni assicurative; b) i dati di programma relativi a circa 8.000 posizioni assicurative caricate nell'archivio informatico; c) il disco chiave di attivazione del programma di gestione degli archivi, riversando tali notizie segrete su personal computer e su dischetti, notizie delle quali si avvaleva l'agenzia privata per conseguire indebito profitto patrimoniale;

— peculato (art. 314 cod. pen.) per essersi appropriato di alcuni dischetti ad alta densità, di cui aveva la disponibilità, dopo avervi registrato programma ed archivio delle posizioni assicurative e di essersi appropriato delle stampe relative alle posizioni di alcuni assicurati clienti dell'agenzia privata;

— abuso d'ufficio in casi non preveduti specificatamente dalla legge (art. 323 cpv. cod. pen.) per avere abusato del suo ufficio, al fine di procurare ingiusto vantaggio patrimoniale all'agenzia privata, acquisendo presso l'Ente pubblico documenti (così qualificati il programma, l'archivio e il disco chiave di accesso) nonché dati relativi alla posizione assicurativa di clienti dell'agenzia, mediante la formazione delle stampe relative ai contributi presenti in varie sedi dell'Ente.

Esito: è stato disposto il rinvio a giudizio.

Osservazioni: nel caso di specie appare interessante sia la formulazione dei reati contestati, sia la qualificazione di documenti data ai programmi e agli archivi informatici.

Caso n. 14.

Fatto: un dipendente addetto all'archivio informatico, procedura ricostruzioni pensioni, ricostruiva alcune pensioni in favore di soggetti non aventi diritto, elevandone l'importo e sostituiva poi, mediante la procedura di correzione dell'elaboratore — che emetteva la cedola di pagamento — il nominativo dell'assicurato con quello di un'altro non avente diritto; quest'ultimo si recava per l'incasso presso l'ufficio postale declinando generalità corrispondenti all'intestatario della cedola esibendo falsi documenti di identificazione. In altri casi il dipendente infedele sostituiva la cedola emessa dall'elaboratore con un'altra nella quale modificava soltanto il nome del beneficiario.

L'azione criminosa è stata scoperta nel 1993 grazie all'impiegato postale, il quale aveva bloccato il pagamento di una cedola perché insospettito dalla consistenza dell'importo e da una telefonata ricevuta la stessa mattina da un anonimo impiegato dell'INPS che chiedeva se vi fossero difficoltà per il pagamento.

Le indagini amministrative hanno scoperto altri casi con avvenuto incasso dell'importo delle cedole.

La denuncia all'A.G. è stata immediata.

Danno: in corso di accertamento.

Stato: sono in corso le indagini da parte della Polizia Giudiziaria con la collaborazione dell'Ispettorato dell'Istituto.

5. ALLEGATO. SISTEMI DI SICUREZZA E PROTEZIONE DEL SISTEMA INFORMATICO DELL'INPS.

Il crescente potenziamento del sistema informatico dell'Istituto, la sempre più diffusa presenza dello stesso sul territorio, i processi di integrazione nella rete delle istituzioni pubbliche e private, hanno reso urgente e indispensabile disporre di un compiuto ed organico sistema di sicurezza e protezione del patrimonio informatico.

A tal proposito sono già in atto misure, sia di carattere organizzativo che tecnico, tendenti a realizzare un primo, significativo passo verso la costruzione di una struttura, controllata dal centro, per costituire un importante deterrente agli accessi ed alle operazioni non autorizzate su aree particolarmente delicate.

Dal punto di vista organizzativo sono state emanate una serie di disposizioni volte a creare una « cornice organizzativa della sicurezza » che, pur tenendo conto della necessaria correttezza degli adempimenti da svolgere e dei livelli di produzione da raggiungere, impongono obblighi specifici in grado di assicurare un significativo passo verso la costruzione di una struttura organizzativa, controllata dal centro, oltre che un importante deterrente agli accessi ed alle operazioni non autorizzate.

Sotto l'aspetto informatico, è stata estesa l'area di protezione dei dati, degli archivi e delle risorse informatiche presso il centro nazionale, ed è stata perfezionata la struttura di delimitazione e separazione delle macro-applicazioni centrali mediante la creazione di « macchine virtuali » dedicate a svolgere funzioni specifiche in un contesto ove risulti più efficace imporre l'utilizzo di flussi informativi standardizzati e controllati.

Inoltre, per applicazioni che investono campi particolarmente critici dal punto di vista della sicurezza, sono state adottate misure che hanno comportato interventi finalizzati, rientranti tuttavia nel disegno strategico del piano globale, assicurando nel contempo un sufficiente livello di protezione.

Un sistema di sicurezza aziendale deve, però, rendere « sicuri » tutti gli elementi costituenti i vari livelli ed diversi componenti del sistema informatico, al fine di proteggerli da eventi non voluti o non previsti, mantenendo nel contempo la flessibilità e la funzionalità del complesso elaborativo; deve cioè inserirsi in un organico piano di strategia globale che investa tutti gli aspetti del sistema, ponendosi diversi obiettivi strategici:

- gestire il rapporto utenti/operatività, adottando per ogni addetto un proprio profilo personalizzato, aggiornabile dinamicamente a seconda delle necessità;

- gestire la riservatezza delle informazioni nei confronti di violazioni non consentite;

- individuare univocamente gli utenti addetti, impedendo accessi non autorizzati al sistema informatico;

- effettuare un monitoraggio delle attività a « rischio » svolte su informazioni ritenute « critiche » da parte di utenti autorizzati, al fine di rendere trasparente l'individuazione di chi ha operato sulle informazioni:

- garantire una completa ed imparziale applicazione della normativa;

- garantire, infine, una flessibilità di ampliamento e di adattamento alle evoluzioni successive derivanti da modifiche tecnologiche, senza introdurre vincoli di carattere tecnico a future scelte organizzative e procedurali dell'Istituto.

Tali obiettivi devono naturalmente essere perseguiti e raggiunti senza intaccare i livelli di produttività dell'Istituto e quindi graduando gli interventi in funzione del livello di criticità delle informazioni e delle operazioni.

Le dimensioni e la complessità del sistema informatico dell'Istituto, sempre più orientato a lavorare con transazioni in « tempo reale », la proiezione verso l'esterno che si sta realizzando in questo periodo, la integrazione dei dati con una capillare rete di telecomunicazioni, la mole e la varietà delle informazioni contenute nelle banche dati hanno portato ad escludere il ricorso a soluzioni parziali e preconfezionate.

L'unica strada che si è ritenuto possibile percorrere è stata quella di utilizzare quanto di meglio offre il mercato in termini di software ed hardware, senza mai rinunciare al coordinamento e alla regia di tutti gli interventi ritenuti necessari, e sviluppando direttamente presso l'Istituto il software e le tecnologie necessarie al mantenimento del controllo di gestione, pur avvalendosi di collaborazioni qualificate, al fine di conseguire il miglior risultato e le sinergie di progettazione necessarie ed indispensabili su progetti di tale entità.

A tale proposito è stata effettuata una lunga attività di studio e di esperienze, di contatti con esperti anche internazionali, di rapporti con centri di ricerca e partecipazione a convegni e seminari specializzati.

Il progetto che ne è scaturito si basa, sostanzialmente, su alcune linee fondamentali:

- la creazione di un doppio livello di sicurezza, uno generalizzato ed uno riservato alle applicazioni con un maggior livello di « criticità »;

- l'utilizzo di meccanismi di controllo legati sia ad elementi di conoscenza (password) che ad elementi di possesso (badge a microprocessore contactless) con relativo lettore;

- installazione, per le stazioni di lavoro, che abbisognano di particolare protezione (responsabili della sicurezza, Direttori di Sede, ispettori di vigilanza, etc.), di apposite schede crittografiche;

- introduzione di schermi software su tutti i livelli del sistema (stazioni di lavoro, sistemi di Sede AS400 ed LSX, sistemi regionali e sistemi centrali), cooperanti interattivamente con le applicazioni e le procedure dell'Istituto;

- registrazione delle operazioni effettuate.

Il monitoraggio dell'intero sistema verrà effettuato da un « sistema esperto », realizzato direttamente all'interno dell'Istituto, con lo scopo di gestire automaticamente le tabelle di sicurezza, controllare gli accessi sia a livello centrale che periferico, monitorare le operazioni a rischio e fornire le indicazioni di auditing e di implementazioni future.

La realizzazione di tale sistema globale di sicurezza sarà necessariamente perseguita attraverso una metodologia di lavoro multifase, il cui svolgimento verrà articolato in diversi stadi di sviluppo e fasi di realizzazione, ognuno dei quali comporterà il raggiungimento di risultati intermedi.

La varie fasi di attività saranno basate su obiettivi che sono in diretta correlazione con la particolare struttura dell'Istituto impostata sul concetto di *centralità del posto di lavoro*: dal posto di lavoro individuale, infatti, vengono avviati i processi elaborativi per fornire servizi all'utenza e vengono modificati i dati dei vari archivi locali, regionali e centrali.

Il primo punto, quindi, per realizzare un efficace sistema di sicurezza, consiste nel proteggere adeguatamente il posto di lavoro mediante l'identi-

ficazione e la registrazione dell'autore che richiede accesso ai servizi informatici (« conoscere chi ha fatto che cosa »).

Generalmente le soluzioni di sicurezza logica si fondano esclusivamente sull'utilizzo di chiavi segrete di accesso (password), note soltanto alla persona autorizzata: questo costituisce una necessità, ma anche un rischio notevole.

Infatti, una volta trafugate le chiavi segrete, il sistema perde la sua prima ed unica linea di difesa contro gli accessi non autorizzati, gli errori e le frodi.

Pertanto è necessario prevedere un ulteriore livello di protezione, che associ alla conoscenza di qualcosa (password) il possesso di qualcosa (tessera personale).

L'insieme inscindibile di questi due elementi elimina totalmente il rischio di accessi non autorizzati al sistema informatico.

Per quanto riguarda le tessere personali (badges) il mercato offre una vasta scelta tra vari tipi e modelli, da quelli a semplice banda magnetica a quelli con memoria e processore autonomi, sui quali è possibile memorizzare una grande mole di informazioni sul « profilo » del possessore.

Tra questo ultimo tipo di carte magnetiche è risultata di particolare interesse quella cosiddetta « contactless », caratterizzata dal fatto di avere memoria e processore completamente affogati nella plastica senza contatti metallici esterni.

Tale metodologia costruttiva elimina ogni rischio di smagnetizzazione, deterioramento, sporcizia e, soprattutto, possibilità di manomissioni volontarie.

Va inoltre aggiunto che le predette carte verranno dotate anche di banda magnetica di identificazione, al fine di poter essere utilizzate anche in funzione di badge per la procedura di rilevazione delle presenze, consentendo di poter fornire al personale un unico strumento idoneo a registrare le presenze e a consentire l'accesso al sistema informatico.

La protezione del posto di lavoro non è però da sola sufficiente a garantire la sicurezza del sistema informatico da errori o frodi volontarie di chi è autorizzato ad operare; non è pensabile che, una volta acceduto al sistema, ognuno possa « navigare » senza restrizioni all'interno delle applicazioni, senza alcuna possibilità di controllo.

Un valido sistema di sicurezza deve essere in grado di controllare e gestire in qualsiasi momento la validità della terna « soggetto-azione-oggetto », deve cioè essere in grado di « pilotare » chi opera sul sistema soltanto verso le applicazioni a lui consentite, e di monitorare in tempo reale tutte le operazioni effettuate su dati considerati a rischio, anche e soprattutto in considerazione della sempre più ampia apertura all'esterno dell'Istituto.

A tale scopo, nonché al fine di rendere flessibile e trasparente tale attività e di consentire una precisa analisi dei flussi informativi, si prevede di inserire un Sistema Esperto — di cui peraltro è già stato sviluppato in Istituto un prototipo — da applicare alla specifica realtà dell'Istituto. Tale sistema, oltre a soddisfare le esigenze suesposte, consente anche di apportare modifiche ed implementazioni fondandosi su una base di conoscenze che si andrà ampliando mano a mano che il sistema stesso funziona. In tal modo verrà realizzata una architettura non statica ma essenzialmente dinamica che permetterà una crescita graduale con gli elementi che costituiscono la catena dei flussi informativi, e che consentirà una ca-

pacità di evoluzione e di adattamento alle situazioni mutevoli senza introdurre vincoli di carattere informatico.

Il sistema di sicurezza, che andrà consolidandosi per gradi successivi, sarà così coordinato e controllato dal sistema esperto, progettato e realizzato *ad hoc*, per le funzioni di monitoraggio del patrimonio informativo dell'Istituto, di controllo dei flussi informativi e degli accessi ai dati ed alle procedure anche al fine di ottenere indicazioni per l'evoluzione delle metodologie di sicurezza, sulla base dell'utilizzo delle informazioni raccolte nella fase operativa.

In definitiva, il sistema esperto sopra delineato verrà a svolgere più funzionalità di base:

- quella di prevenzione, finalizzata a rendere il sistema impenetrabile, integrata con il sistema di controllo degli accessi a cui fornisce le regole di gestione dei profili e delle autorizzazioni relative;

- quella di controllo e allarme, finalizzata alla diagnosi precoce delle situazioni potenzialmente critiche, con capacità di rilevare ed evidenziare le irregolarità sulla base di soglie statistiche e vincoli procedurali.