Articolerò il mio intervento su pochi punti:

- preliminarmente, fornirò alcuni dati sulle potenzialità della rete e sulle linee di tendenza verso cui stiamo muovendo;
- evidenzierò, poi, i più rilevanti elementi di contesto esterno, rimarcando i punti di contatto tra *cyber security ed* economia digitale;
- prima delle conclusioni, farò, infine, un breve *excursus* sull'organizzazione della Guardia di Finanza in materia di contrasto alle illegalità commesse via *Internet*, inserendovi sintetiche considerazioni con riguardo a due tra le maggiori fenomenologie illecite.

1. PREMESSA: POTENZIALITÀ DELLA RETE E LINEE DI TENDENZA

In questi ultimi anni abbiamo assistito ad una rapida evoluzione nell'utilizzo delle tecnologie collegate ad *Internet* che ha prodotto un costante aggiornamento dei modelli di interazione e, conseguentemente, di acquisizione dei servizi e dei beni da parte dei cittadini, delle imprese e delle Pubbliche Amministrazioni. Si è affermato, così, un nuovo modo di vivere, organizzare l'impresa, lavorare e governare la *res publica*.

Nel nostro Paese, secondo i più aggiornati dati *Audiweb (marzo 2014)*, sono 35,6 milioni gli italiani attivi sulla Rete.

Siamo di fronte ad una vera e propria esplosione sociale e culturale, oltre che tecnologica, di determinati fenomeni legati, soprattutto, all'accesso *on-line* ai servizi. Questa rivoluzione vede la prepotente avanzata dell'utilizzo dei dispositivi cd. *mobile*.

Sono, infatti, 7,4 milioni gli italiani che accedono ad *Internet* solo da *mobile* (il 37% degli utenti *online* nel giorno medio), mentre 5,3 milioni solo da PC. L'uso combinato riguarda 7,2 milioni di cittadini. Tra questi il 91% degli utenti tra i 18 ed i 24 anni si può definire *multiscreen surfer*, con una forte propensione all'uso esclusivo dei dispositivi mobili per accedere ad *Internet*.

Sui dispositivi mobili vanno per la maggior parte *social network*, siti o applicazioni legate al mondo dei cellulari.

I dati sulla crescente importanza del mondo del *mobile* sono confermati anche dai numeri dell'*advertising*, in costante crescita su tali canali.

In tal senso va letto anche il fatto che, a partire dal 2012 il mercato del PC sta registrando cali costanti, -9.5% nel 2013, mentre nel 2014, probabilmente per via della necessità di provvedere alla sostituzione delle vecchie macchine che lavorano ancora con *Windows XP*, la flessione dovrebbe essere molto inferiore, intorno al 2,4%.

A fine 2014 *smartphone* e *tablet* raggiungeranno, insomma, rispettivamente, in Italia, quota 45 e 12 milioni (Osservatorio *Mobile & App Economy* del Politecnico di Milano). La ricerca mostra come lo sviluppo di ecosistema *mobile* generi effetti rilevanti in chiave economica: 1 *mobile surfer* su 3 ha scaricato applicazioni a pagamento sul proprio dispositivo, 1 su 5 ha acquistato almeno un prodotto o servizio, 4 su 5 interagiscono con la pubblicità attraverso questi *device* e 1 dispositivo su 2 verrebbe utilizzato anche come strumento di pagamento al posto della carta di credito. Per dare dei valori economici si consideri che il *Mobile Commerce* che ora vale 1,2 miliardi di euro, si stima possa arrivare a valere oltre 7 miliardi

di euro nel 2016, con un peso relativo sull'*e-commerce* che, se oggi è pari al 12%, potrebbe, sempre nel 2016, superare il 40%. Così come ancora nel 2016 il mercato dei pagamenti *mobile* potrebbe valere, complessivamente 6 miliardi di euro.

Come ho anticipato, il grosso dei ricavi sugli 1,2 miliardi di *App* scaricate dagli italiani negli ultimi 12 mesi arriva dalla pubblicità (+167% nell'ultimo anno rispetto agli 1,4 miliardi di euro nel 2012).

La portabilità e la comodità propria di questi oggetti rendono, inoltre, sempre più diffusi i casi di "*dual use*", cioè di utilizzo ibrido dello stesso dispositivo, tipicamente in ambito privato e *business* introducendo vulnerabilità nuove da gestire all'interno delle organizzazioni di tipo imprenditoriali e, di conseguenza, nelle relazioni di tipo economico.

Circa la vulnerabilità dei sistemi mobili, è possibile attendersi che attraverso tali dispositivi potranno essere realizzati attacchi sempre più sofisticati ed aggressivi, dal momento che oltre ad avere ormai potenza di calcolo e di connettività di tutto rilievo, nella maggior parte dei casi gli utenti non li dotano di protezioni anti-*malware* efficaci, anzi, spesso, sono loro stessi a manometterli per sbloccarne alcune funzionalità avanzate, rendendoli ancora più vulnerabili.

Il secondo elemento di forte novità sulla Rete è l'attivismo delle generazioni più giovani.

Uno studio commissionato da *Eurispes* per il 2012 dimostra come, oggi, oltre il 23% dei ragazzi fra gli 8 ed i 12 anni navighi in *Internet*

per un’ora al giorno, il 32% addirittura per circa 2 ore ed il 23% per oltre due ore al giorno. Ciò in misura sempre maggiore attraverso *smartphones* e *tablet* che sono nella loro disponibilità in maniera massiccia già a partire dai 9 anni di età.

Quasi sempre questa ultima tipologia di strumenti è vista dai più giovani utilizzatori come semplici “*gadget*”, consentendo, così, agli attaccanti di sfruttarne le caratteristiche peculiari (geolocalizzazione sopra tutte) per compiere nuovi tipi di crimini, anche molto insidiosi. In questo contesto, è opportuno sottolineare come l’elevata diffusione di tali *device*, tra i giovani ed i giovanissimi, porterà inevitabilmente ad un aumento dei reati perpetrati contro questa fascia di popolazione.

Va aggiunto, poi, che se il processo di educazione digitale dei cittadini appare ancora difficoltoso, lo stesso non si può dire per i *Cyber* criminali che escogitano, invece, metodi di offesa sempre più sofisticati ed aggressivi, in grado di influenzare i comportamenti degli utenti anche dal punto di vista psicologico, con danni apprezzabili per l’*Internet economy* nazionale.

Un esempio emblematico di come queste forme di criminalità possano influenzare il comportamento degli utenti è rappresentato dal *virus* conosciuto come “*ransomware*” apparso, anche nel nostro Paese, da più di due anni e capace di ingannare l’utente facendogli credere di essere incappato in un falso sequestro, da remoto, del PC da parte della Guardia di Finanza o di altra Forza di Polizia, a causa della presenza sullo stesso di contenuti illeciti a carattere osceno. Ovviamente, i finti agenti di Polizia, si premurano di rappresentare come con il pagamento, rigorosamente *on line*, di una “multa” possa risolvere il problema evitando guai di natura giudiziaria.

Un attacco di questa natura, nei cui confronti, nello scorso anno, grazie alla cooperazione internazionale coordinata da *Europol*, è

stata data una prima, importante, risposta, dimostra, come l'utilizzo di fattori offensivi, che fanno leva su vulnerabilità di tipo tecnologico, ma soprattutto culturali ed emotive dell'utente, possa produrre effetti dissuasivi importanti circa l'utilizzo dei servizi offerti dall'*online*, con ricadute negative sulla crescita dell'economia digitale.

L'osservazione di questa realtà mostra, infatti, come le più recenti sfide del crimine informatico siano rivolte al mondo dei *Social Network*, che spingono l'utente ad esporre eccessivamente la propria identità digitale. Questi rischi aumentano in maniera esponenziale nei confronti degli utilizzatori di dispositivi mobili, posto che è più difficile distinguere una pagina *web* contraffatta su uno schermo di ridotte dimensioni.

Tutte le citate criticità sono acuite da specifici fattori, quali:

- la generale mancanza di *know-how* in materia di *Internet Technology* da parte dei responsabili aziendali;
- la bassissima consapevolezza degli utenti finali;
- le peculiarità intrinseche dei dispositivi mobili, più difficilmente riconducibili all'interno delle *policy* e dei sistemi di controllo esistenti in ogni Organizzazione.

Un cenno, per l'importanza e l'attualità della materia (mi riferisco, da ultimo, alla recente normativa che ha introdotto per le partite IVA l'obbligo di ricevere pagamenti sopra i 30 euro con il POS) voglio dedicarlo all'utilizzo, nel nostro Paese, dei mezzi di pagamento elettronici ed all'impiego di mezzi alternativi al contante.

Quanto al primo aspetto, si può osservare come, in Italia (fonte Banca d'Italia), nel 2012 siano state effettuate circa 70 operazioni *pro capite* con mezzi di pagamento diversi dal contante (assegni, bonifici, addebiti, carte di pagamento), a fronte delle oltre 180 registrate in media nell'Eurosistema (più di 170 nei Paesi UE-27).

Altri Paesi, che hanno una maggiore tradizione rispetto a questi strumenti di pagamento, presentano medie di molto superiori, come ad esempio la Finlandia, con più di 400 operazioni per abitante.

Nonostante ciò, anche per l'Italia è rilevabile una crescente diffusione degli strumenti di “moneta elettronica”.

Complessivamente, ad oggi, le carte di pagamento che circolano nel nostro Paese sono circa 70 milioni (contro i 28 milioni del 1998) ed i relativi possessori ammontano ad oltre 25 milioni, pari al 40% della popolazione nazionale complessiva.

Quando ho accennato ai cosiddetti mezzi alternativi al contante, intendevo, invece, riferirmi all’introduzione su larga scala di tecnologie che consentono agli utenti di effettuare micropagamenti tramite dispositivi portatili.

Si tratta, nello specifico:

- della tecnologia NCF (*Near Field Communication*). Al momento, comunque, i POS abilitati in Italia a ricevere pagamenti via NFC, che è attivo sui sistemi *Android,* sarebbero solo il 10%;
- degli applicativi di *Apple* e *Google* che hanno puntato sui *wallet* virtuali nei quali si registrano i dati delle proprie carte di credito, che vengono utilizzati selezionando un'apposita *app*;
- della possibilità di effettuare il pagamento fotografando, con lo *smartphone*, il QR di un oggetto.

Alcune aziende offrono, infine, al cliente, al momento del pagamento *on line*, la possibilità di premere un tasto cd. “*My Bank*” per accedere, immediatamente, al proprio *home-banking* abituale e confermare l’acquisto in modo automatico inserendo le proprie *password*. Le maggiori banche italiane stanno fornendo tale soluzione a imprese, Enti pubblici e clienti privati in tutta Italia, anche per pagamenti in Europa.

In merito, poi, al fenomeno “criptomoneta” che sta assumendo dimensioni di portata globale, condivido personalmente l’esigenza avanzata da molti esperti di prevederne una regolamentazione, magari leggera. Nello specifico, sarebbe importante poter ricondurre la titolarità dei portafogli elettronici ad una identità certa, anche legata ad un “*Personal Identification Number*” rilasciato da una Pubblica Autorità. Solo in tal modo, potrà crescere il livello di fiducia della generalità dei cittadini verso innovazioni che contribuiscono alla crescita dell’economia digitale nel suo complesso e solo così potrà ridursi il rischio che questi strumenti vengano utilizzati per finalità illecite.

2. ELEMENTI DI CONTESTO ESTERNO

Dalla seconda metà dei primi anni duemila, il tema della *cyber-security* anche in campo economico ha acquisito una rilevanza crescente per l’Unione Europea. Non poteva essere diversamente, se si pensa che l’economia digitale europea ammonta, oggi, a oltre 1.100 miliardi di euro l’anno. Ne è dimostrazione, tra l’altro, il dinamismo delle Istituzioni europee, a vari livelli. Basti citare, sul punto, la costituzione nel 2004 dell’Agenzia Europea per la Sicurezza delle Reti e dell’Informazione (*European Network and Information Security Agency*, ENISA), la nascita nel 2013, in ambito Europol, dello *European Cybercrime Centre*, ovvero l’attenzione che Olaf e Commissione Europea (ove insiste anche, nell’Ufficio per l’Armonizzazione del Mercato Interno, l’Osservatorio Europeo sulle violazioni dei diritti di proprietà intellettuale) hanno messo sulla sicurezza economica e finanziaria delle imprese, dei cittadini e delle Pubbliche Amministrazioni.

Quanto all’Italia con il DPCM 24 gennaio 2013, in data 18 dicembre 2013, sono stati adottati dal Presidente del Consiglio dei Ministri il Quadro Strategico Nazionale ed il Piano Nazionale per la sicurezza cibernetica del Paese con i quali vengono trattati i profili e le tendenze evolutive delle minacce alle reti ed ai sistemi informatici

d’interesse nazionale, nonché individuati gli strumenti e le procedure da adottare per il contrasto a queste attività criminali, attribuendo specifici compiti ai vari soggetti pubblici e privati coinvolti.

Anche all’interno del mondo delle imprese l’argomento digitalizzazione, negli ultimi anni ha assunto un’importanza crescente. Esso rappresenta, infatti, da un lato un fattore fondamentale per aiutare la crescita delle aziende, dall’altro un possibile vantaggio nell’implementare strategie competitive, determinanti per oltrepassare questo periodo di stallo dell’economia europea, quali, ad esempio, processi di riorganizzazione aziendale e di internazionalizzazione.

L’innovazione costituisce, infatti, un volano per superare il rallentamento dell’economia, creando nuove opportunità di occupazione, incrementando la crescita e le esportazioni (soprattutto grazie alla diffusione dell’*e-commerce*), fino ad influenzare positivamente la misura del PIL dell’intera Nazione.

Nel panorama europeo l’Italia si pone oggi come Paese inseguitore, con un ruolo dell’economia digitale ancora inferiore rispetto ad altre nazioni, quali Svezia, Gran Bretagna, Francia e Germania. Tuttavia il ruolo delle ICT nel nostro Paese è in espansione e, soprattutto, rappresenta una via obbligata per la crescita, grazie alle enormi opportunità offerte da *Internet* per famiglie, imprese e Pubblica Amministrazione.

Anche la P.A., con un profondo cambio di mentalità, ha sviluppato, ed incentivato l’utilizzo di strumenti tecnologici con il fine di semplificare il rapporto burocratico tra Cittadino e Pubblica Amministrazione.

Una recente ricerca commissionata a Formez PA dal Dipartimento per la Digitalizzazione della PA, in collaborazione con l’Istituto Piepoli ha evidenziato che, sebbene l’operatore dello sportello

rimane il preferito dal cittadino (41%), un 37% degli intervistati ricorre ai servizi *on-line* ed il 18% lo farebbe se fosse dotato di connettività.

E' emerso, inoltre, che l'utilizzo della PEC per comunicare con la PA stenta a decollare (soltanto il 9% del campione intervistato ne ha attivata una).

Anche lo *spread* digitale che il Paese manifesta ha un costo, che, secondo il Censis, è pari a 10 milioni di euro al giorno di minori investimenti in reti, tecnologie e servizi innovativi.

Sempre secondo il Censis, infatti, se nel nostro Paese si sviluppasse il commercio *online* e l'uso della moneta elettronica fino a raggiungere i livelli medi europei, e se si riuscisse a razionalizzare le banche dati della PA centrale, si renderebbero disponibili per nuovi investimenti in reti, tecnologie e servizi innovativi 3,6 miliardi di euro all'anno, ovvero i menzionati 10 milioni al giorno.

Quanto all'economia digitale in senso stretto, nel 2009 il suo valore a livello mondiale poteva essere stimato, secondo McKinsey, in circa 1.672 miliardi di dollari, pari al 2,9% del PIL mondiale[1], oggi si parla già di oltre 4000 miliardi di dollari.

L'incidenza dell'economia digitale varia, tuttavia, significativamente a seconda dei Paesi considerati: sempre nel 2009 negli Stati Uniti contava per il 3,8% del PIL, in Giappone per il 4%, in Cina per il 2,6%. In Europa, le quote appaiono comprese tra il 6,3% della Svezia e l'1,7% dell'Italia.

Malgrado l'impatto economico della digitalizzazione risulti ancora non elevato nel nostro Paese, le cifre sono in crescita: infatti, stime riferite al 2011, a cura di *Boston Consulting Group*, indicano in circa 32 miliardi di euro il valore dell'economia digitale in Italia, con un

[1] McKinsey Global Institute (2011), "Internet matters: The Net's sweeping impact on growth, jobs and prosperity". Lo studio prende in considerazione in particolare le 13 economie più importanti al mondo: Svezia, Germania, Regno Unito, Francia, Stati Uniti, Corea del Sud, Canada, Italia, Giappone, India, Cina, Brasile, Russia.

peso sul PIL pari al 2,5%. A parità di condizioni in termini di consumi privati, investimenti e spesa istituzionale, l'*internet economy* varrà 59 miliardi di euro nel 2015, con un peso sul PIL pari al 3,3%, e una crescita media annua del 13% rispetto al 2009.

Se da un lato, quindi, il confronto con le altre economie avanzate evidenzia lo stato di arretratezza dell'Italia sul fronte della digitalizzazione, dall'altro tale stato suggerisce come vi sia ancora un ampio margine di miglioramento per la diffusione dell'*internet economy* nel nostro Paese.

Ad esempio, le imprese attive nel commercio elettronico in Italia sono, complessivamente, il 5% del totale, contro il 22% della Germania, il 19% del Regno Unito e l'11% della Francia (la media europea è del 14%).

3. GUARDIA DI FINANZA: RUOLI, COMPITI IN MATERIA E POTENZIAMENTO

La Guardia di Finanza, in ogni sua espressione operativa, si muove sempre trasversalmente nell'ambito della missione istituzionale che gli è affidata quale polizia finanziaria sui fronti della lotta all'evasione e del controllo delle uscite, ovvero quale polizia economica nella tutela del mercato dei capitali e di quello dei beni e servizi, oltreché nel contrasto alla criminalità organizzata, soprattutto sotto il versante patrimoniale.

In linea con tale approccio, il Corpo, anche nel contrasto agli illeciti di carattere economico e finanziario realizzati in *Internet*, ovvero attraverso le cd. nuove tecnologie, interviene attraverso due direttrici che sono in continuo contatto funzionale tra loro:

- ✓ la rete dei Reparti territoriali, capillarmente distribuiti sul territorio nazionale, con il compito di assicurare, nei rispettivi ambiti, l'efficiente tutela di tali funzioni. Tra questi i Nuclei di Polizia Tributaria si pongono come Unità investigative di punta;

- ✓ i Reparti Speciali che si affiancano ai primi e che, istituiti per l'investigazione in specifiche materie, sono incaricati di realizzare direttamente, ovvero con azioni di supporto alle Unità operative, moduli investigativi connotati da elevati standard qualitativi per i Reparti territoriali.

I nostri moduli d'azione, anche nelle investigazioni che impattano con il mondo digitale sono, quindi, contestualmente orientati:

- ✓ al controllo economico del territorio virtuale, attraverso il monitoraggio della rete telematica, per verificare l'esistenza di sacche d'illegalità;
- ✓ ad intercettare i flussi finanziari "sospetti" mediante la tecnica cd. "follow the money";
- ✓ a verificare la posizione fiscale dei soggetti investigati per l'eventuale tassazione dei proventi leciti ed illeciti sottratti all'imposizione;
- ✓ ad intervenire, trasversalmente, su altri profili di rilievo, quali, ad esempio, quelli in materia di reati contro la Pubblica Amministrazione, valuta, concorrenza e mercato, Privacy e sicurezza delle comunicazioni.

In tale ambito, al Nucleo Speciale Frodi Tecnologiche, inquadrato nel Comando Reparti Speciali, sono affidati, a livello nazionale, compiti di polizia giudiziaria, di analisi, di supporto, di studio e formazione, nonché responsabilità nelle relazioni istituzionali di tipo operativo.

L'attività di servizio è sviluppata nel solco dei citati compiti di polizia economico/finanziaria e, in un'ottica di efficace sinergia interforze, nei comparti di specializzazione o, comunque, nei settori d'intervento rimessi alla competenza del Corpo dal decreto del Ministro dell'Interno approvato il 28 aprile del 2006. Mi riferisco, in particolare, alla tutela dei movimenti dei capitali e dei mezzi di

pagamento, nonché alla salvaguardia dei marchi, dei brevetti e della proprietà intellettuale.

Il Corpo, nell'ultimo biennio, ha, inoltre, rinforzato le capacità operative che nel comparto informatico esprimono le proprie Unità territoriali e le varie componenti dei Reparti Speciali, attraverso la costituzione, presso i Nuclei di Polizia Tributaria, sull'intero territorio nazionale, di apposite Unità dedicate ai compiti di "*Computer Forensics* e *Data Analysis*", cui sono stati assegnati militari avviati a specifici corsi di formazione che vengono, annualmente, tenuti presso la Scuola di Polizia Tributaria. Questa rete di specialisti sarà sempre più in coordinamento funzionale con le Unità Speciali del Corpo, secondo una logica che, con riferimento ad indagini caratterizzate da elevato spessore tecnologico, oltreché multidistrettualità e/o sovranazionalità, pone queste ultime come punto di riferimento dei terminali sul territorio.

4. CRIMINALITÀ E CYBER CRIME

In campo economico/finanziario gli interessi del cyber-crime sono, particolarmente, elevati verso settori quali le frodi bancarie, il furto di identità e di informazioni, la contraffazione, l'evasione fiscale sul commercio elettronico, la pirateria digitale ed i giochi e le scommesse on line. Ciò provoca danni patrimoniali ingenti ai privati in termini di minore occupazione, alle aziende minandone la capacità reddituale ed all'economia pubblica riducendo la base imponibile delle imposte dirette e indirette e, quindi, il gettito fiscale complessivo del Paese.

Riguardo all'impatto del cybercrime sull'economia digitale, una ricerca Norton del 2012 valuta in 2.45 miliardi di euro il costo dei crimini informatici contro gli utenti consumer in Italia. Rispetto allo scorso anno, come ampiamente detto, ed in linea con il forte sviluppo dei nuovi settori digitali, sono in aumento i casi associati ai social network e ai dispositivi mobili, mentre è diminuito il costo per

ogni vittima (complessivamente sarebbero circa 9 milioni le persone colpite dal crimine informatico, il 25% del totale degli utenti attivi in Italia).

Sul punto, un breve cenno intendo riservarlo a due tra le fenomenologie illecite sull'*online* più insidiose: mi riferisco ai temi della contraffazione ed a quello del *gaming* illegale.

Il primo, infatti, che non coinvolge solo *fashion* e *luxury goods* – si pensi alla vendita attraverso questi canali di pezzi di ricambio per automezzi ed elettrodomestici, a quella di giocattoli o di prodotti la cui commercializzazione è riservata a canali regolamentati (come i farmaci) – produce conseguenze particolarmente gravi sia per l'affidabilità delle transazioni, sia per i titolari dei diritti di proprietà industriale violati, sia, soprattutto, per la sicurezza e la salute degli utenti.

Rispetto ai contraffattori tradizionali, i siti *Internet* di commercio elettronico, e specialmente quelli che si limitano a commerciare *online*, senza spazi fisici accessibili dai consumatori, rendono più difficile distinguere i prodotti veri da quelli falsi, spesso semplicemente riprodotti con immagini "ufficiali", tratte dai cataloghi del produttore.

In tale ambito il Corpo ha messo in campo insieme ai Dicasteri dell'Interno e dello Sviluppo Economico, il S.I.A.C., Sistema Informativo Anti Contraffazione.

Si tratta di una progettualità finanziata dalla Commissione Europea ed affidata, per la sua realizzazione e gestione, alla Guardia di Finanza, a conferma del ruolo centrale del Corpo nello specifico comparto.

Il S.I.A.C., in particolare, è un applicativo informatico che opera, dal 1° gennaio scorso, su una piattaforma *web* e si articola in una serie di funzioni, alcune delle quali riservate alle Unità operative del

Corpo ed alla collaborazione con le forze di polizia e gli altri Organismi che agiscono sul fronte anti-contraffazione.

Le funzionalità in argomento consentono la raccolta strutturata dei dati delle operazioni di servizio effettuate sul territorio, allo scopo di agevolare le analisi di rischio sulle modalità di attuazione delle condotte illecite e sulle dinamiche dei fenomeni, per meglio orientare gli interventi di contrasto.

A breve, il sistema sarà completato da un ulteriore applicativo volto al monitoraggio dei canali di distribuzione di merci *on line*.

Con riferimento al secondo settore la nostra esperienza operativa dimostra, in particolare, come sulla rete vi sia stata una proliferazione di siti che, proponendosi come veri e propri casinò virtuali, consentono agli utenti di accedere alle più disparate offerte di gioco, in assenza di qualsiasi autorizzazione. Si tratta di risorse *web* solitamente allocate su "*server*" ubicati in territorio estero.

Noto a tutti, al riguardo, è il forte interesse che la criminalità organizzata ha manifestato, sin dall'inizio, nel controllo di queste filiere di gioco clandestino in virtù dei guadagni "esentasse" che il gioco illecito consente e della possibilità di reinvestire denaro di dubbia provenienza.

Al di là dei profili di carattere penale che tali vicende assumono, per arginare la diffusione del gioco abusivo via Internet, l'AAMS, oltre a prevedere per i concessionari già autorizzati la possibilità di raccogliere giocate anche attraverso l'ausilio dei mezzi telematici, così da riportare nel circuito legale, i giocatori attratti dal "web", ha adottato, in collaborazione con la Guardia di Finanza, una specifica procedura di carattere amministrativo finalizzata alla inibizione, tramite il loro "oscuramento", dei siti che propongono giochi non autorizzati. Dal 2006 ad oggi sono oltre 5000 i siti individuati ed inibiti sulla base di questa attività.

5. CONCLUSIONI

Internet, in definitiva, come tutte le tecnologie innovative, è una realtà incontestabile in termini di progresso e di democrazia. Basti pensare, ad esempio, alla quantità di informazioni che oggi troviamo liberamente sulla rete, anche di carattere giuridico, tecnico, societario, finanziario etc. etc.. La ricerca di queste informazioni fino ai primi anni '90 impegnava molta parte del nostro tempo ed era anche molto costosa visto che comportava l'impiego di risorse umane e finanziarie. Un altro innegabile vantaggio si ritrova nella estrema facilità di comunicare e scambiarsi, in piena legalità, notizie, documenti o immagini. Come sempre, allora, la patologia risiede nell'utilizzo illegale della tecnologia e non nelle capacità che questa ci offre.

Internet come fonte aperta rappresenta, inoltre, un'opportunità per gli Organismi di *Law enforcement*; non sono rari, infatti, i casi investigativi risolti attraverso elementi trovati sulla rete.

Le nuove tecnologie sono, in sostanza, un formidabile ausilio per combattere i fenomeni criminali che infestano la Rete, a patto che, tra gli attori che operano nella legalità e per la legalità, si mantengano strette forme di collaborazione e cooperazione.

Ecco perché il Corpo, ha tenuto, da sempre, una linea di collaborazione con gli Enti nazionali ed internazionali che hanno compiti di controllo, regolamentazione e prevenzione, nei vari comparti della nostra missione istituzionale, oltreché con le maggiori associazioni di categoria, come testimoniato anche dai numerosi Protocolli d'intesa in atto.

I Reparti del Corpo si avvalgono, così, nell'ambito della loro azione di ricerca, prevenzione e repressione degli illeciti di polizia economico/finanziaria commessi nel mondo virtuale, ovvero attraverso le nuove tecnologie, della conoscenza "dall'interno" che su tali fenomeni hanno i Soggetti che operano istituzionalmente nel

settore a tutela dei cittadini, delle imprese e dell'economia nazionale ed europea.

Voglio ricordare, infine, che il recentissimo meeting "Digital Venice 2014", svoltosi nella città lagunare alla presenza del Presidente del Consiglio dei Ministri italiano e del Commissario UE per l'Agenda Digitale si è chiuso riconoscendo l'importanza delle competenze digitali per la creazione di posti di lavoro e la crescita della competitività, nonché affermando che l'economia digitale è il punto di partenza per un nuovo sviluppo economico attraverso le *start up* come potenziali motori per la crescita, il mercato unico digitale, la connettività, i nuovi servizi e la digitalizzazione della Pubblica Amministrazione.

La crescita poggia, allora, su queste basi ed il compito di un Corpo di Polizia economico-finanziaria, quale è la Guardia di Finanza, è quello di garantire, anche nel contesto virtuale, il rispetto delle regole per fornire un fattivo contributo allo sviluppo dell'Italia ed un concreto sostegno all'imprenditoria onesta.