Anno XXVIII numero 1 – febbraio 2019

Periodico quadrimestrale a cura dell'Ordine degli Avvocati di Parma.
Autorizzazione del Tribunale di Parma n.14 del 10 giugno 1992.

Spedizione in abbonamento postale
art. 2 comma 20/c legge 662/96
Filiale di Parma
Direttore responsabile:
avv. Giuseppe Negri

Cronache dal Foro Parmense

SOMMARIO

chiuso in redazione il *9 maggio 2019*

Comitato di redazione (ante)

avv. Nicola Bianchi, avv. Angelica Cocconi, avv. Emanuela De Roma, avv. Alessandra Mezzadri, avv. Giovanni Nouvenne, avv. Lucia Silvagna

Comitato di redazione (post)

INTERNI
avv. prof. Luigi Angiello avv. Simona Cocconcelli avv. Angelica Cocconi Avv. Matteo Mancini

ESTERNI
avv. Nicola Bianchi avv. Alberto Magnani

Hanno collaborato a questo numero

Matteo Cavalieri (immersio.eu)
Simona Cocconcelli
Giannandrea Garau (cripton.it)
Amerigo Ghirardi
Romualdo Gobbo (b.digital)
Luca Guiggi (omnigrade.it lawonchain.io)
Alberto Magnani
Girolamo Marazzi (blueit.it)
Lorenzo Negri (cripton.it)
Pietro Pettenati
Lucio Riva (Barilla group)
Giovanni Tortorici (Barilla group)
Giacomo Voltattorni

Sfide e opportunità

EDITORIALE

di Simona Cocconcelli

Il nuovo Consiglio dell'Ordine che ho l'onore di presiedere si è da poco insediato e mi trovo a riflettere sulla professione di Avvocato nella società dinamica e tecnologica di oggi.
Quali le sfide e le opportunità ?

La prima sfida è quella di riportare il ruolo e la funzione dell'avvocato ai livelli ancora più alti per autorevolezza, dignità e professionalità. E proprio Piero Calamandrei diceva che: "L'avvocatura è una professione di comprensione, di dedizione e di carità". E questo oggi rimane immutato, ma non basta più, perché l'avvocato dev'essere anche tecnologico, informatizzato e continuamente aggiornato e preparato sulle ultime novità informatiche, dinamico e collegato con altri avvocati, organizzato e pronto a sperimentare. Infatti, la possibilità di avere accesso alle nozioni e notizie, tramite la rete, amplifica la conoscenza in tutti i campi lavorativi e aumenta la velocità con cui si acquisiscono le informazioni che interessano e si eseguono ricerche; il risultato è certamente un vantaggio per tutti, ma per l'Avvocato significa anche un rialzo dell'asticella, nel senso che a parità di informazione accessibile anche al cliente, la qualità del suo intervento professionale si misurerà esclusivamente sulla preparazione giuridica e segnatamente sulla capacità di inquadrare le varie fattispecie per arrivare ad una soluzione del caso.

La tecnologia e le sue innovazioni futuristiche sono già qui. Negli ultimi dieci anni sono intercorsi numerosi cambiamenti nella nostra vita quotidiana e professionale, dall'obbligatorietà della PEC, alla firma digitale, l'accesso ai servizi polisweb, l'introduzione degli smartphone, i servizi on-line quali Airbnb, Uber, Amazon, sino alle App, ai navigatori sempre più dettagliati, alla tv interattiva, fino a Google Home e così via. Tutte queste novità tecnologiche hanno sconvolto silenziosamente il nostro mondo, nell'economia, nella vita e così nel diritto. Vi sono sempre più dettagliate discipline a tutela dei dati sensibili (ai sensi del GDPR 679/2016), anche per l'antiriciclaggio ed anticorruzione, nuove norme di diritto internazionale privato sugli scambi commerciali telematici, le determinazioni sul cloud computing o sul crowdfunding, ma si dovrà poi regolamentare anche l'utilizzo di robot con intelligenza artificiale e la macchina con autopilota. Il diritto ha seguito – seppure in ritardo – tutte queste rivoluzioni.

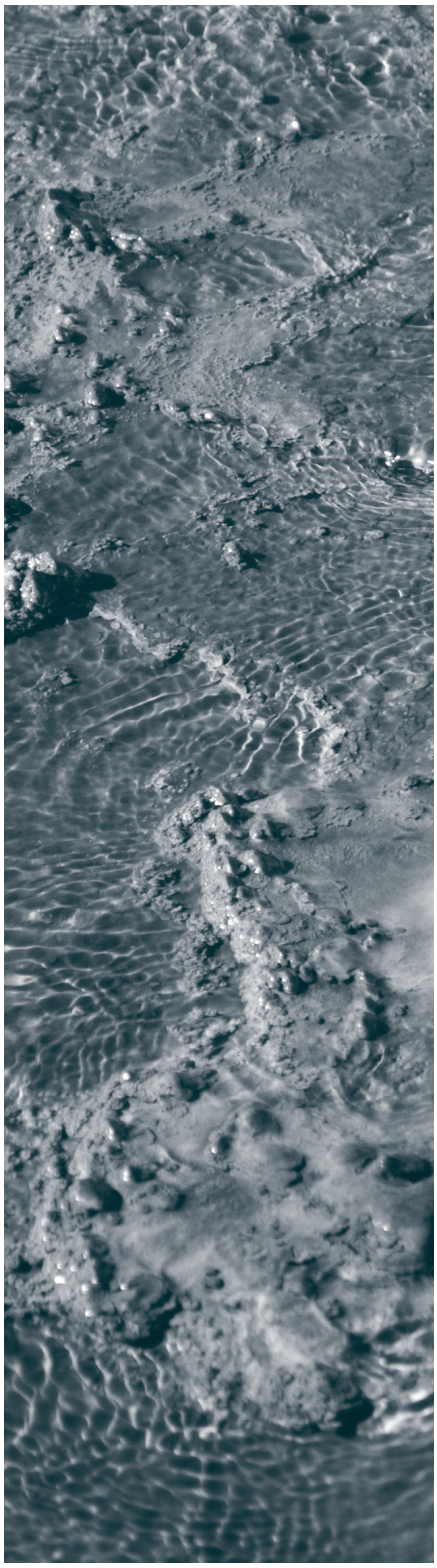
Questo sicuramente migliorerà l'efficienza nella vita quotidiana e negli studi legali, ma porterà in generale anche problemi di privacy, di tracciabilità e di controllo da parte di terzi. E non solo per ciò che riguarda la sfera ristretta privata o professionale, ma più in grande l'ambito pubblico per la sicurezza nazionale e di garanzia dei servizi.

Ognuna delle cose citate comporta implicazioni etiche e di diritto che andranno risolte da qui ai prossimi dieci, venti trent'anni. Uno dei problemi è che la velocità dell'innovazione non corrisponde alla velocità del Diritto e del relativo aggiornamento normativo. La produzione di leggi e regolamenti è lenta e complessa: se non evolverà, sarà inadeguata a far fronte alle esigenze della società del futuro. Ed inoltre, il legislatore di oggi sta lavorando per limitare la giurisdizione e così modificare il processo (sia civile che penale, per arrivare a quello amministrativo e tributario) ed il ruolo del legale.

Noi Avvocati siamo chiamati, a tutti i livelli, a scongiurare di non arrivare troppo tardi. Dovremo studiare e prepararci a fare i consulenti delle nuove tecnologie, comprendere prima degli altri i problemi e risolverli.

Il futuro nella lingua greca antica aveva un antico valore desiderativo per esprimere l'attesa di qualcosa che sarà, ma che si sta vivendo oggi nel presente. Ebbene, proprio come i greci antichi, vi esorto a non chiedervi come sarà il futuro perché il futuro è già qui. Nessuna domanda, c'è solo da viverlo ed affrontarlo. E nel caso delle nuove tecnologie, con tutte le implicazioni giuridiche ed etiche del caso, occorre avere il coraggio di studiarle e riconoscerle. E così una volta vissuta l'esperienza, ricorrerete anche voi al presente o all'*aoristo* ed al perfetto per raccontarlo a vostra volta, perché avrete compreso le fattispecie 4.0 (smart contracts, blockchain, cyber security, operazioni di scambio in bitcoin...e così via) e potrete portare avanti l'esperienza nei nuovi ambiti del diritto, per non perdere nessuna delle occasioni che sono già intorno a Noi.

Tecnologie che trasformano



Oltre all'impatto sociale portato dalle nuove tecnologie, sempre più consapevolmente si pone il tema degli aspetti legali della tecnologia quale argomento di studio e di impegno professionale.

La redazione ha individuato alcuni operatori economici impegnati nelle tecnologie più avanzate i quali, in alcuni casi assistiti dai loro legali, hanno saputo descriverci le aree di maggiore interesse ed impatto anche per la professione forense (intelligenza artificiale[1], blockchain, bitcon, cybersecurity, smart contract, realtà virtuale ed aumentata): ci hanno offerto materiali derivanti dalla loro esperienza che descrivono "IL" fenomeno tecnico che oggi influenza in modo sempre più pervasivo il mondo, e con esso la pratica dell'avvocatura e della giustizia: la digitalizzazione.

Prodotti e servizi sono dematerializzati in quanto vengono realizzati e fruiti senza un supporto fisico: documenti di qualsiasi genere, filmati, musica, servizi bancari, servizi della pubblica amministrazione, ecc. .

Una volta che i dati sono informatizzati è possibile utilizzarli in modo strutturato con sistemi informatici di ricerca, valutazione, rielaborazione da parte degli utenti attraverso software o servizi on-line: un caso consueto per i giuristi è quello della ricerca dei precedenti giurisprudenziali.

Gli archivi dei dati, arricchiti di elementi rilevanti, sono soggetti anche ad utilizzi più avanzati nei quali, rimanendo all'esempio della ricerca giurisprudenziale, il dato ricercato non è più soltanto il dato letterale (ricerca testuale) ma anche il suo significato nella realtà (ricerca semantica) con un notevole incremento di utilità (e facilità d'uso diretto da parte di soggetti non tecnici).

Con sistemi sempre più evoluti si arriva a funzioni che sono svolte direttamente dai computer sfruttando i dati a seguito di un semplice impulso di ricerca[2].

Un altro aspetto della digitalizzazione è il fatto che i dati sono pronti per la condivisione in collaborazione fra persone distanti: posta elettronica anche certificata, messaggistica istantanea, software/servizi per il lavoro di gruppo, svolgimento di attività on-line con condivisione video e documenti, i webinar[3] della formazione a distanza, ecc. .

Tutto ciò ha aperto in passato scenari ai quali siamo ormai abituati ma che, ugualmente, non smettono di generare novità degne di approfondimento e nuove implicazioni giuridiche nelle quali, giorno dopo giorno, ci imbattiamo.

La valutazione di quali sono i temi nuovi spetta a ciascuno di noi valutando la propria esperienza, un punto di partenza minimo può essere il domandarsi quanto segue:

- la detenzione dei dati è legittima?
- a chi appartengono i dati?
- chi ha dei dati un legittimo diritto di uso/detenzione?
- come proteggere i dati?
- come dare la prova legale dei dati?

Per quanto non esista un settore del diritto privo di ricadute, le discipline giuridiche di più immediato riferimento sono il diritto della proprietà intellettuale ed il diritto della tutela dei dati personali.

Quanto alla proprietà intellettuale: la nascita del dato, la sua appartenen-

1 **Chatbot:** un robot che dialoga in tempo reale con un suo interlocutore per rispondere alle domande di cittadini e utenti. **Diagnosi medica.** Rientrano nelle intelligenze artificiali i sistemi automatici di diagnostica che refertano la malattia di una persona leggendo gli esiti di esami sulla base delle statistiche condotte su grandi quantità di dati (si arriva a strumenti predittivi per valutare potenziali rischi di evoluzione delle malattie individuali). **Insegnamento.** Sono già operativi sistemi di valutazione dei compiti scolastici in grado di seguire gli studenti singolarmente, proponendo loro contenuti specifici. **Sicurezza pubblica.** *Computervision* e *natural language processing* per individuare minacce in tempo reale (videosorveglianza). **Controllo assenze dei lavoratori.** Un algoritmo, elaborato dall'Inps, ma la cui applicazione è stata sospesa, incrocia i certificati medici con altri dati contenuti Inps (come la retribuzione individuale), e crea liste di lavoratori da sottoporre a visita medica sulla base di un modello predittivo. **Giustizia.** Esperienze di giudici robot sono presenti in alcune giurisdizione.

2 Esempi relativi al diritto degli Stati Uniti https://techindex.law.stanford.edu/, https://rossintelligence.com/.

3 Webinar ("seminario interattivo tenuto su Internet").

za originaria4 o derivata, la sua circolazione (cessione diritti, licenze) se il dato deve essere tenuto riservato perché non perda il suo valore[5] o su quali specifici accorgimenti deve fondarsi la sua protezione[6].

Quanto al tema della tutela dei dati personali, spesso percepito come un aggravamento ingiustificato di formalità non sempre utili, dalla legge 675 del 1996 che qualche "documento legale" ancora vediamo citare, si sono susseguiti studi di ogni genere e lo sviluppo di questo settore è sotto gli occhi di tutti soprattutto dopo l'entrata in vigore del Codice della Tutela dei Dati Personali[7] nell'ormai lontano 1.1.2004 e del Regolamento Comunitario c.d. GDPR[8] in data 25.5.2018 tanto che alcuni economisti che hanno affrontato frontalmente il tema in modo evoluto hanno formato un tipus professionale e sono definiti come "privacy economist"[9].

I temi che leggerete nei contributi suggeriscono un continuo divenire fra nuove possibilità tecniche ed altrettanto nuove conseguenze da valutare dal nostro punto di vista.

Gli approcci dei Paesi sono molto diversi: a proposito di uno dei temi più importanti, l'intelligenza artificiale[10], la Commissione Europea ha formato un gruppo di 52 esperti (High Level Expert Group on Artificial Intelligence) che dovrebbe emettere le linee guida per gli algoritmi proprio quando Google, nove giorni dopo averlo nominato, ha già chiuso il comitato di esperti che avrebbe avuto il compito di consigliare l'azienda sulle modalità di uso, eticamente corrette, dei propri sistemi di intelligenza artificiale.

Questo significa che non sarà così facile intervenire con "regole" in questo settore.

Al momento in Italia leggiamo la sentenza del Consiglio di Stato n.2270/2019 nella quale, a proposito di un meccanismo automatizzato di indicizzazione di domande amministrative, così ha statuito "Il meccanismo attraverso il quale si concretizza la decisione robotizzata -ovvero l'algoritmo- deve essere «conoscibile», secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico. Tale conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti. Ciò al fi ne di poter verificare che gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare – e conseguentemente sindacabili – le modalità e le regole in base alle quali esso è stato impostato. In altri termini, la «caratterizzazione multidisciplinare» dell'algoritmo (costruzione che certo non richiede solo competenze giuridiche, ma tecniche, informatiche, statistiche, amministrative) non esime dalla necessità che la «formula tecnica», che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella «regola giuridica» ad essa sottesa e che la rendano leggibile e comprensibile, sia per i cittadini che per il giudice.".

I contributi hanno lo scopo di sollecitare ciascuno di noi nel meglio comprendere le nuove possibilità di impegno professionale per essere sempre il punto di riferimento in un mondo che cambia.

Alberto Magnani [11]

4 Art. 12-bis Legge 633/1941 "*Salvo patto contrario, il datore di lavoro è titolare del diritto esclusivo di utilizzazione economica del programma per elaboratore o della banca di dati creati dal lavoratore dipendente nell'esecuzione delle sue mansioni o su istruzioni impartite dallo stesso datore di lavoro" – Art. 64 D.Lgs.30/2005 "1. Quando l'invenzione industriale è fatta nell'esecuzione o nell'adempimento di un contratto o di un rapporto di lavoro o d'impiego, in cui l'attività inventiva è prevista come oggetto del contratto o del rapporto e a tale scopo retribuita, i diritti derivanti dall'invenzione stessa appartengono al datore di lavoro, salvo il diritto spettante all'inventore di esserne riconosciuto autore … omissis …".*

5 Per esempio la pre-divulgazione del contenuto di una domanda di brevetto che, ai sensi dell'art. 46 del D.Lgs. 30/2005, fa perdere il requisito della novità all'invenzione e, quindi, la validità dell'eventuale brevetto.

6 Decreto legislativo del 10/02/2005 - N. 30 Art. 98 - Oggetto della tutela. 1. Costituiscono oggetto di tutela i segreti commerciali. Per segreti commerciali si intendono le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni: a) siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore; b) abbiano valore economico in quanto segrete; c) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete. 2. Costituiscono altresì oggetto di protezione i dati relativi a prove o altri dati segreti, la cui elaborazione comporti un considerevole impegno ed alla cui presentazione sia subordinata l'autorizzazione dell'immissione in commercio di prodotti chimici, farmaceutici o agricoli implicanti l'uso di nuove sostanze chimiche. Art. 99 – Tutela 1. Ferma la disciplina della concorrenza sleale, il legittimo detentore dei segreti commerciali di cui all'articolo 98, ha il diritto di vietare ai terzi, salvo proprio consenso, di acquisire, rivelare a terzi od utilizzare, in modo abusivo, tali segreti, salvo il caso in cui essi siano stati conseguiti in modo indipendente dal terzo. 1-bis. L'acquisizione, l'utilizzazione o la rivelazione dei segreti commerciali di cui all'articolo 98 si considerano illecite anche quando il soggetto, al momento dell'acquisizione, dell'utilizzazione o della rivelazione, era a conoscenza o, secondo le circostanze, avrebbe dovuto essere a conoscenza del fatto che i segreti commerciali erano stati ottenuti direttamente o indirettamente da un terzo che li utilizzava o rivelava illecitamente ai sensi del comma 1. 1-ter. La produzione, l'offerta, la commercializzazione di merci costituenti violazione, oppure l'importazione, l'esportazione o lo stoccaggio delle medesime merci costituiscono un utilizzo illecito dei segreti commerciali di cui all'articolo 98, quando il soggetto che svolgeva tali condotte era a conoscenza o, secondo le circostanze, avrebbe dovuto essere a conoscenza del fatto che i segreti commerciali erano stati utilizzati illecitamente ai sensi del comma 1. Per merci costituenti violazione si intendono le merci delle quali la progettazione, le caratteristiche, la funzione, la produzione o la commercializzazione beneficiano in maniera significativa dei suddetti segreti commerciali acquisiti, utilizzati o rivelati illecitamente. 1-quater. I diritti e le azioni derivanti dalle condotte illecite di cui ai commi 1, 1-bis e 1-ter si prescrivono in cinque anni.

7 D.Lgs.196/2003

8 Regolamento Ue 2016/679

9 https://www.ted.com/talks/alessandro_acquisti_why_privacy_matters?language=en

10 "Secondo le previsioni dell'Agid (l'Agenzia per l'Italia digitale https://www.agid.gov.it/it/agenzia) tra cinque anni l'intelligenza artificiale sarà in grado di tradurre simultaneamente il linguaggio parlato, fra trent'anni un robot potrà scrivere uno dei bestseller selezionati dal New York Times e tra quarant'anni potrà sostituire l'uomo in ogni attività." Marino Longoni prima pagina di "Italia Oggi" del 15.4.2018

11 Ringrazio Nicola Bianchi per avere voluto realizzare questo approfondimento ed avermi coinvolto nel trovare contributori esperti. Ringrazio tutti gli autori dei singoli pezzi perché hanno investito, con il loro tempo, nell'avvocatura di Parma, e non solo, confermando come nell'osmosi fra competenze diverse, le loro e le nostre, risieda l'interesse di tutti.

sui frequenti anglicismi

Cari Colleghi,
il vostro vecchio redattore ha sempre posto cura attenta ai testi (spesso consultando il prezioso sito dell'Accademia della Crusca) per sostituire in bell'idioma i sempre più frequenti anglicismi, così forzando talora le intenzioni degli autori, od almeno usando corsivi e virgolette per evidenziare e distinguere.

Ma in questo numero un poco speciale ha dovuto gettare la spugna.

Troppi, per nulla superflui e poco sostituibili, per la sintesi e la forza relazionale che esprimono, sono anch'essi segno dei tempi e ancor più del futuro.

Che restino strumenti di una comprensione comune e d'un linguaggio globale com'è il mondo e non diventino idoli di metallo fini a se stessi, capaci anche di distoglierci dalla verità della nostra missione e funzione sociale.

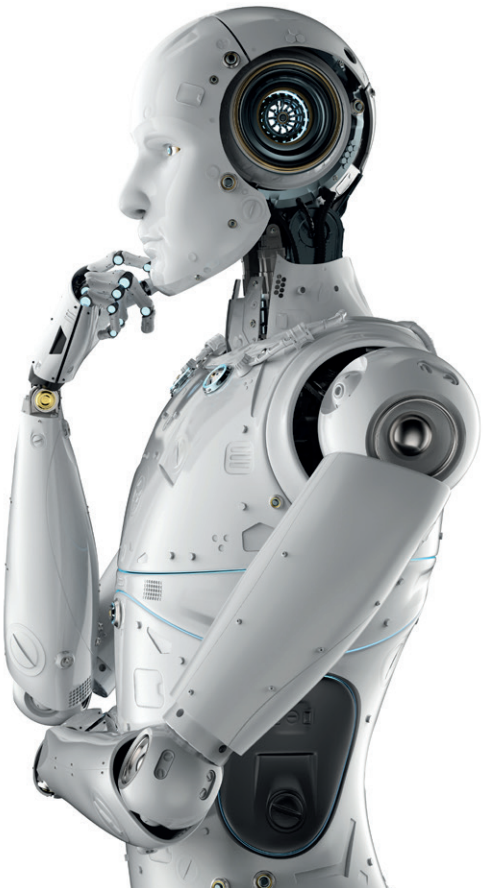
Il contributo dell'Intelligenza Artificiale nell'ambito legale

Il contributo dell'Intelligenza Artificiale nell'ambito legale.

In b.digital il laboratorio di innovazione della Blueit di Monza fra le linee guida per lo sviluppo delle applicazioni in modalità innovativa vi è il "Cognitive" che ricopre un ruolo avanzato nel panorama delle soluzioni basate sull'Intelligenza Artificiale (IA).

Nell'ambito del "Cognitive" si collocano tutte quelle applicazioni che hanno la capacità di auto addestrarsi (Deep Learning) e per le quali il mondo della ricerca sta sperimentando strutture sempre nuove che si basano sulla composizione del cervello umano simulando neuroni e sinapsi nelle cosiddette "reti neurali".

Il processo di addestramento consiste nel fornire un flusso di informazioni continuo, quali ad esempio immagini di insetti nelle più svariate combinazioni di luce di ambiente o altro, per poi verificare se la rete si è auto addestrata per riconoscere comunque una combinazione di immagini mai vista prima, così come succede ad un bambino che riconosce un tipo di animale mai incontrato (ad es. un cane) per similitudine con quelli che già conosce. Essere guidato nell'apprendimento è compito dei genitori che lo aiutano a discernere sempre con maggior attenzione le caratteristiche peculiari di quanto appreso ed è proprio in questo senso che vengono proposte alla rete neurale immagini sempre nuove perché rafforzi ed affini la sua conoscenza.



In b.digital abbiamo sperimentato direttamente questo tipo di soluzioni quando nel 2017 abbiamo partecipato al contest mondiale lanciato da IBM con l'iniziativa Watson Build, dove si richiedeva di sviluppare una applicazione che includesse le tecnologie IA del loro sistema Watson.

Con bioBotGuard, l'applicazione da noi scelta per individuare gli insetti nocivi nei campi di patate a partire da delle riprese fotografiche effettuate da un drone, siamo diventati nel Novembre 2017 geo-champion, utilizzando proprio questa capacità straordinaria di individuare la Dorifora (l'insetto nocivo delle patate), grazie alla funzione "Visual Recognition" di Watson.

Sono comunque molteplici le declinazioni della IA in funzione dei sistemi e dei metodi di addestramento, sotto la quale ritroviamo pianificazione, comprensione del linguaggio (NLP-Natural Language Processing), il già citato riconoscimento di immagini (Visual Recognition), riconoscimento di oggetti (Object Detection) e suoni, riconoscimento di pattern, ecc. fra i quali risulta di sicuro interesse l'interpretazione del linguaggio scritto nell'ambito di un dominio ben preciso come quello legale.

Già siamo utilizzatori quotidiani dei motori di ricerca per il recupero di contenuti tramite frasi o parole chiavi (full-text search) che ci forniscono risultati straordinari basati sull'analisi delle correlazioni presenti nei testi memorizzati, ma grazie all'IA il riconoscimento del testo non si ferma solo alla mera interpretazione della scrittura, anche manoscritta, risolta da tempo da sistemi OCR (Optical Character Recognition) ormai d'uso comune, ma alla estrapolazione dal testo dei significati indotti (intenti) specifici del dominio applicativo a cui il testo si riferisce.

Relativamente a quest'ambito l'aiuto della IA contribuisce a catalogare i documenti non solo sulla base della semantica derivata dal loro contenuto, ma classificandoli per la loro natura "emotiva" derivata dal tono con cui il documento è stato stilato (tone, sentiment analysis).

Esperienza specifica in tal senso è stata in b.digital la classificazione di documenti come contratti o lettere di rimostranza, per le quali l'IA ha contribuito a definire non solo la caratteristica specifica del documento, come ad es. rilevare che un documento è il contratto originario, un rinnovo contrattuale o appartiene alla classe dei documenti integrativi, ma anche classificare le lettere ricevute come lettere di rimostranza a vari livelli di importanza proprio per il "tono" con cui vengono stilate.

Gli strumenti messi a disposizione per questo tipo di classificazione avanzata, sono strumenti informatici evoluti che hanno necessità di essere addestrati con casi d'uso specifici in modalità "supervisiona-

ta" (Supervised Learning), ossia si insegna al sistema a riconoscere determinate casistiche di documenti dandogli in pasto un significativo numero di documenti dai quali derivare o meglio "inferire" (qui risiede l'aspetto "intelligente") classificazioni simili così come farebbe un classificatore umano.

In questo tipo di esperienza è stato particolarmente illuminante riclassificare documenti precedentemente classificati, non essendovi più il vincolo temporale del procedimento dell'uomo, e scoprire gli errori di classificazione, condizione che rende questa tipologia di applicazioni particolarmente efficace e garantita.

I documenti sono di fatto classificati dai sistemi intelligenti tramite l'analisi correlata delle informazioni derivate dal contenuto che si concretizza con l'attribuzione di una etichetta ("tagging") che sintetizza la natura della classificazione come ad es. contratto, lettera o altro, ma l'aspetto interessante di questa attribuzione è che può andare anche al di là del mero contenuto potendo essere la stessa etichetta risultato e fonte di informazioni. Si pensi ad es. alla ricerca di documenti relativi ad un argomento classificato come "militare" derivato perché i documenti analizzati trattano di soldati, colonnelli o altro.

La nostra esperienza nell'utilizzo della IA nell'ambito legale si è limitata all'automatismo di una classificazione intelligente documentale, ma grandi player come IBM e non solo, stanno proponendo servizi, sviluppati con i medesimi strumenti software da noi utilizzati, orientati al supporto dei professionisti del settore:

https://www.ibm.com/blogs/client-voices/save-the-lawyer-ai-technology-accelerates-and-augments-legal-work/

L'esperienza maturata nell'utilizzo della IA negli ambiti su citati, ci ha resi consapevoli degli aspetti da considerare per non ripetere gli errori non solo nella scelta della tecnologia IA da utilizzare, ma anche e soprattutto nelle modalità di utilizzo, in un approccio sempre di supporto all'azione umana.

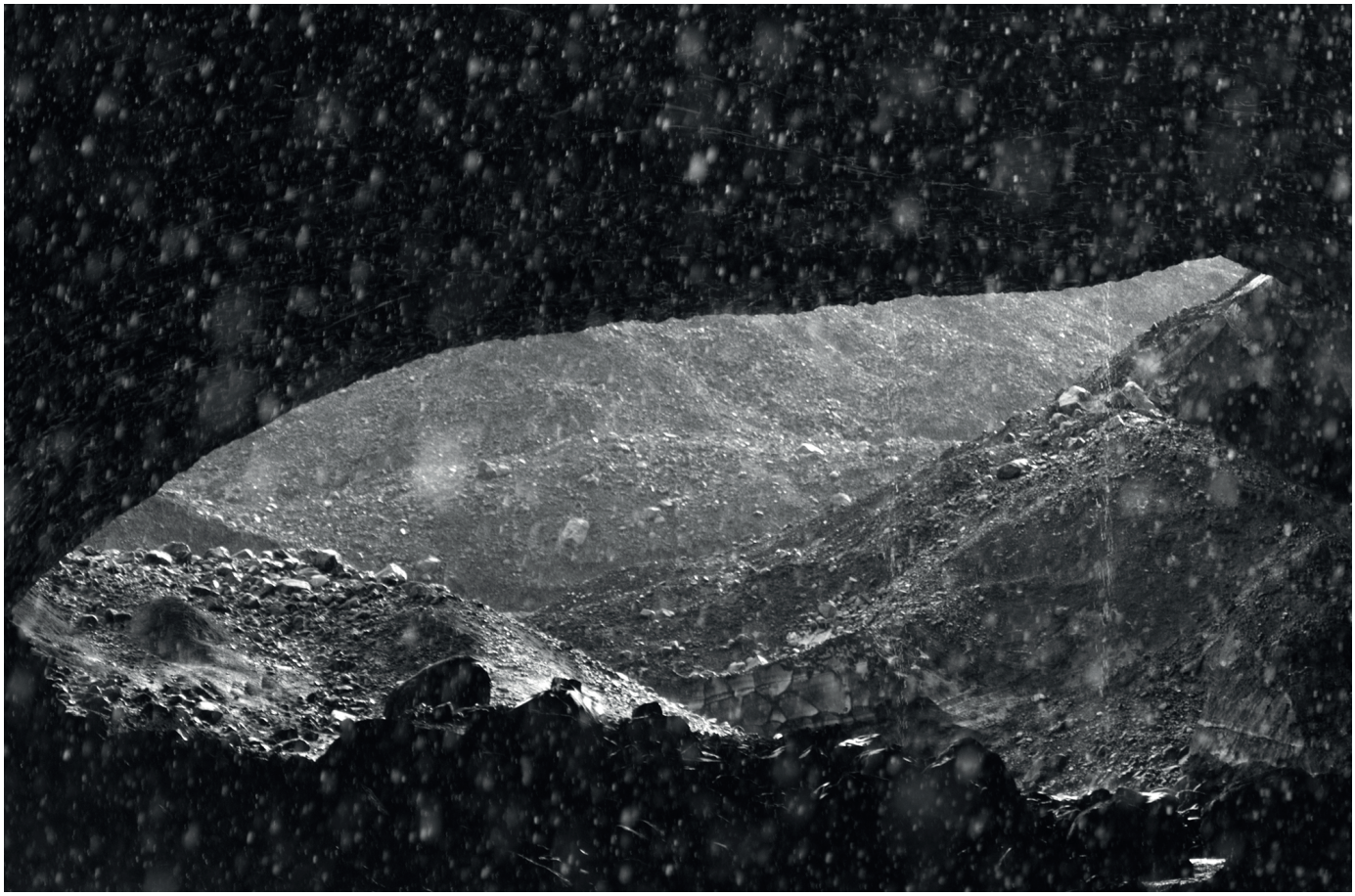
Questa consapevolezza ci ha portato a progettare in un modo nuovo le applicazioni dove la componente di IA, la parte intelligente, svolge le funzioni di un assistente che propone all'utente scelte già ragionate sulla base dell'esperienza maturata di utilizzo dell'applicazione sviluppata.

Un assistente "intelligente" ad es. si può far carico di raccogliere informazioni preliminari per risolvere un caso tecnico (ticket) anticipando ad esempio al proprio utente parte della sua attività, con evidente risparmio di tempo e maggior efficacia nella risoluzione del caso.

Con questo approccio in Blueit stanno nascendo nuove proposte applicative di "robotizzazione" delle procedure, che non ho timore a dire che possano essere proposte anche nell'ambito legale, contribuendo a migliorare qualità e tempestività di esecuzione.

Girolamo Marazzi
CEO BlueIT Group

Romualdo Gobbo
Presidente b.digital



Introduzione alla Blockchain

"Tutti sanno che una cosa è impossibile da realizzare
finché arriva uno sprovveduto che non lo sa e la inventa"
Albert Einstein

Questa serie di articoli, non costituisce un trattato informatico, ma appare su un periodico dell'avvocatura di Parma che dedica un numero alla tecnologia blockchain.

E' però necessario percorrere qualche nozione tecnica per apprezzare e meglio comprendere questa rivoluzione alla quale noi informatici stiamo assistendo da vicino. Rivoluzione che però non riguarda solo noi ma una vasta porzione del mondo delle imprese umane.

Lo scopo è quello di spiegare quali siano le vere potenzialità di questa tecnologia che cambierà e per certi versi, ha già cambiato, le relazioni tra persone e cose.

Vorremmo farlo cercando di essere il più semplici possibili e allo stesso tempo restituire il vero significato e il vero valore della tecnologia di cui stiamo per parlare.

Spesso le informazioni riguardanti la blockchain sono frammentate, erronee, imprecise nel migliore dei casi. Ci piacerebbe quindi approfittare di questa opportunità, per fare conoscere l'intimo aspetto della tecnologia blockchain, convinti che, al di là degli slogan, o come si dice da qualche tempo, degli hashtag, ci sia effettivamente un valore che può essere colto ed utilizzato per rendere migliori i rapporti e le comunicazioni tra le persone.

Non a caso nel 2018 appena conclusosi, sono diverse decine gli stati che hanno indirizzando iniziative mirate allo sviluppo delle tecnologie tra le quali si è recentemente imposta anche la blockchain.

Blockchain che, come vedremo fa la sua comparsa nel 2008, come tecnologia di ausilio alla creazione dei Bitcoin, in risposta alla grossa crisi mondiale originata dal caso Lehman Brothers.

Il bisogno o meglio il problema, a cui il leggendario (e mitologico) inventore di Bitcoin (Satoshi Nakamoto) ha voluto rispondere creando appunto i Bitcoin e donando indirettamente all'umanità i principi della tecnologia blockchain organizzati in modo ordinato, è stato quello di rendere impossibile, (o per lo meno molto più difficile) il rischio di "double spending" della moneta.

Per ottenere questo risultato, è stato creato un sistema che consente la disintermediazione delle transazioni, da entità centrali, (che ne esercitano quindi il controllo), permettendo scambi di valore punto-a-punto, grazie all'adozione di transazioni crittografate, basate su processi di fiducia distribuita.

Dunque, la volontà di non avere più bisogno della presenza di un'entità centrale, (istituzione), è stato il boost iniziale allo sviluppo di Bitcoin e poi, appunto, della blockchain.

Blockchain nasce dunque con l'idea di essere uno strumento di ausilio in ambito finanziario, ma è sempre più evidente quanto le sue caratteristiche possano essere adatte in ambiti applicativi differenti.

Vedremo più avanti anche alcuni esempi di applicazioni della tecnologia blockchain in nell'ambito legale.

Preme qui ricordare come vengano alla ribalta due termini che non si incontrano spesso: decentralizzazione (del valore) e disintermediazione.

La decentralizzazione consentirà la nascita di nuovi sistemi di comunicazione, basati sullo scambio di valore. Non serve un'entità centrale che certifichi e pertanto sarà difficile avere manipolazione o corruzione, banalmente perché non ci sarà più nessuno da corrompere e difficilmente si riuscirà a manipolare un dato che non è più presente in un solo luogo ma è distribuito tra più nodi, replicato uguale a se stesso migliaia di volte.

Ci sentiamo quindi di poter affermare che anche il settore legale assisterà a incredibili cambiamenti guidati dalla tecnologia. Qualcuno sostiene che nei prossimi 15 anni, in questo settore, se ne vedranno di più di quante non se ne siano vista negli ultimi 200 anni.

Quanto sopra è sicuramente vero in scenari di diritto anglosassone, dove il regime legale particolarmente liberalizzato, ha consentito il lancio di strutture di business "alternative" (pensiamo ad esempio alla risoluzione di dispute online), ma si attendono anche da noi novità dal punto di vista legislativo, che potranno aprire le porte a nuove iniziative del tutto attualmente inimmaginabili: probabilmente dunque, emergeranno nuovi metodi di fornire servizi legali.

Il mondo legale avrà pertanto necessità di adattarsi: si stanno diffondendo sempre più i sistemi di reputazione online, nei quali i clienti condividono il loro parere circa il livello dei servizi ricevuti dallo studio presso il quale si sono rivolti. (una sorta di tripadvisor rivolto al mondo legal).

Sistemi di comparazione dei prezzi, e vere e proprie aste on line, mirate alla vendita di quei servizi che sono pacchettizzabili perché ripetitivi.

La blockchain è fondamentalmente un nuovo paradigma per l'organizzazione delle attività, con meno attrito e maggiore efficienza e ad un livello di scala superiore rispetto a quello dei paradigmi attuali: la tecnologia blockchain offre una portata universale e globale ad un livello prima impossibile.

Luca Guiggi

Partner
Amministratore Delegato
www.omnigrade.it

Blockchain e Bitcoin

https://bitcoin.org/bitcoin.pdf

Come menzionato nell'introduzione, non ci sarebbe blockchain senza bitcoin.

E' sembrato quindi naturale che questo paragrafo si intitolasse con il nome del white paper pubblicato nel 2008 dal misterioso personaggio che si firma Satoshi Nakamoto.

Costui, è la persona o l'organismo che avrebbe organizzato in maniera ordinata tutta una serie di tecnologie già esistenti, per ideare Bitcoin come mezzo di pagamento distribuito e trustless e la struttura di registri distribuiti sulla quale Bitcoin si appoggia.

Ci si riferisce a tale struttura con il nome di blockchain.

Nessuna delle principali idee sottostanti Bitcoin e blockchain erano originali, ma il merito di Nakamoto è stato quello di organizzarle secondo un'architettura che risolveva alcune importanti tematiche nella progettazione e ideazione di un sistema decentralizzato utile ai pagamenti.

Il fatto importante è stato quello di organizzare la blockchain utilizzando una classica rete peer-to-peer in cui ciascun partecipante opera come "nodo" e distribuisce o utilizza l'informazione, decentralizzandola.

Inoltre introduce un meccanismo di consenso, di cui parleremo più avanti, che ha il duplice scopo di incentivare i "nodi" a condividere potenza di calcolo, e contemporaneamente a creare un interesse da parte loro a fare in modo che non vi siano comportamenti poco chiari.

Per ultimo ma non per importanza, l'utilizzo della crittografia a chiave asimmetrica che garantisce univocità e integrità agli scambi e ai messaggi che originano sulla blockchain.

Questo mix di ingredienti sono combinati assieme da Nakamoto per dare origine al protocollo di comunicazione e registro non modificabile che chiamiamo blockchain.

Focus: crittografia

La crittografia è una branca della matematica che viene spesso utilizzata in ambito di cybersicurezza.

Etimologicamente significa "scrittura segreta", ma la la crittografia include molto più che una "scrittura segreta".

La crittografia può essere usata ad esempio, per provare di essere a conoscenza di un segreto senza dover rivelare quel segreto (firma digitale), o provare l'autenticità di una serie di dati (impronta digitale).

Il possesso di criptovaluta (ad esempio bitcoin) è attribuito attraverso una chiave digitale, un indirizzo (bitcoin), e una firma digitale. Le chiavi digitali non sono salvate sulla blockchain ma vengono detenute dall'utente in un file o un database, che viene chiamato wallet (portafoglio). Le chiavi sono sempre distribuite a coppie: una privata(segreta) e una chiave pubblica, generate l'una dall'altra. Possiamo pensare alla chiave pubblica come al numero di conto corrente (non c'è alcuna controindicazione a che questo sia conosciuto da tutti), mentre la chiave privata la possiamo associare al PIN che consente di avere il controllo su quel conto.

Un wallet di criptovaluta è un insieme di coppie di chiavi pubbliche e

private. La chiave privata è un numero, normalmente generato in modo casuale, dal quale si genera la chiave pubblica, che a sua volta è il punto di partenza per generare un indirizzo di criptovaluta. Ad un indirizzo di criptovaluta corrisponde quindi una sola chiave privata che attraverso la crittografia (asimmetrica), "firma digitalmente" una transazione e genera una firma numerica. Questa firma numerica può essere generata solo da qualcuno che conosce la chiave privata. La crittografia asimmetrica rende possibile per chiunque verificare ciascuna firma su ciascuna transazione, rendendo certo che solo i possessori di chiavi private valide possono generare firme valide.

2. Conosciamo la blockchain

Per poter capire la tecnologia blockchain forse vale la pena accennare ai sistemi distribuiti, essendo la blockchain prima di tutto un sistema distribuito.

I sistemi distribuiti sono dei paradigmi di calcolo nei quali due o più nodi (per semplificare immaginiamo dei server) collaborano assieme in modo coordinato per ottenere il medesimo risultato.

Esempio: il motore di ricerca Google è un grosso sistema distribuito, che all'utente appare come un'unica piattaforma.

Un nodo è il singolo attore del sistema distribuito, e ciascuno è in grado di scambiare messaggi con gli altri. Un nodo può essere integro, malfunzionante, o malevolo. Un nodo che esibisce comportamenti irrazionali viene indicato con il nome di nodo Bizantino, dal noto problema dei generali Bizantini.

Secondo questo problema, un gruppo di armate bizantine comandate da diversi generali sta decidendo se attaccare o ritirarsi dall'assalto ad una città.

Siccome le truppe sono schierate in modo tale che i generali non riescano a comunicare a voce, l'unico modo di farlo è attraverso lo scambio di messaggi, in modo che siano concordi nello sferrare l'attacco al fine di vincere la battaglia. Il problema risiede nel fatto che potrebbero esserci alcuni dei generali che sono dei traditori e quindi veicolare un messaggio non corretto. E' dunque necessario un meccanismo che consenta di raggiungere l'accordo tra i generali pur in presenza di possibili generali traditori.

In analogia con i sistemi distribuiti, i generali possono essere considerati come i nodi, (i traditori come nodi Bizantini (malevoli), e il messaggero può essere considerato come il canale di comunicazione tra i generali.

Per farla breve il problema si risolve utilizzando un algoritmo di fault tolerance, nel quale il consenso viene raggiunto dopo che si sono ricevuti un certo numero di messaggi contenenti il medesimo contenuto firmato.

A questo punto siamo pronti per cercare di dare una definizione di blockchain o catena a blocchi (chain of blocks) come inizialmente chiamata dal suo ideatore.

La blockchain è un registro distribuito peer-to-peer, crittograficamente sicuro, nel quale si può solo aggiungere contenuto (append-only), immutabile e aggiornabile solo attraverso un meccanismo di consenso raggiunto tra i diversi peer.

Al fine di migliorare la comprensione, vediamo i termini della definizione uno a uno.

Registro distribuito: è in un registro (un supporto sul quale vengono registrati dei dati), che viene suddiviso tra più nodi della rete. Nel caso della blockchain, la suddivisione del registro è su tutti i nodi. Ciascun nodo detiene una copia completa del registro e non esiste una copia originale.

Peer-to-peer: questo termine indica il fatto che non esiste un controllo centrale della rete e ciascun nodo, parla con gli altri direttamente. Questa proprietà consente l'esecuzione di operazioni o di pezzi di codice, tra i vari nodi senza che ci sia necessità di coinvolgimento di una terza parte.

Crittograficamente sicuro: significa che è stata utilizzata la crittografia (asimmetrica) per fornire servizi che fanno in modo che questo registro sia al sicuro dalla falsificazione e/o da un uso scorretto. Questi servizi garantiscono l'integrità del dato e l'origine dello stesso.

Append-only: i dati possono solo essere aggiunti in stretto ordine cronologico. Questa proprietà implica che una volta che il dato è stato aggiunto alla blockchain, è di fatto impossibile che venga cambiato. Ciò consente di considerare immutabile tale dato. (esistono degli scenari teorici rari, in cui in modo molto difficile e al costo di dover corrompere il 51% della potenza di calcolo della catena, è possibile modificare i dati).

Esistono anche situazioni legittime (preconfigurate ad esempio dal GDPR) tipo il "diritto all'oblio" in cui è giustificata l'adozione di soluzioni eleganti al fine di modificare i dati contenuti nei blocchi.

Al di là di quanto sopra, e in tutti i casi pratici, la blockchain è immutabile e il contenuto non può essere alterato.

Aggiornabile attraverso consenso: per ultimo vediamo questo attributo che è il più critico di tutto l'impianto tecnologico e introduce il concetto di consenso, che tratteremo più avanti. Il consenso è ciò che attribuisce la caratteristica della decentralizzazione alla blockchain, nel senso che non c'è alcuna autorità centrale che controlli o sovraintenda all'aggiornamento del registro. Al contrario, ogni aggiornamento è validato attraverso stretti criteri definiti dal protocollo della blockchain e l'aggiornamento è effettuato solo dopo che sia stato raggiunto un consenso tra tutti i nodi della rete. Per ottenere il consenso ci sono vari algoritmi che assicurano che tutti i nodi siano d'accordo sullo stato finale dei dati sulla blockchain.

A questo punto possiamo introdurre il concetto di ***blocco***. Un blocco è semplicemente una collezione di transazioni assemblate assieme ed organizzate logicamente.

Una transazione è la registrazione di un evento, ad esempio la registrazione del trasferimento di denaro da un emittente ad un beneficiario. Un blocco è fatto di diverse transazioni e la sua dimensione varia a seconda del tipo di blockchain in uso.

Nel blocco è sempre inserito un legame con il blocco precedente in modo che sia sempre ricostruibile la catena degli eventi procedendo a ritroso.

L'unica eccezione a quanto sopra è

costituita dal primo blocco, il quale, come è ovvio, non può avere riferimenti relativi a blocchi precedenti.

3. Benefici e limiti della blockchain

Fatte le presentazioni, è utile analizzare brevemente quali siano i benefici ed elencare i limiti di questa tecnologia.

Tra i benefici va ricordata innanzitutto la decentralizzazione. Come già detto, questo è un concetto centrale e un aspetto molto importante della blockchain. Non c'è necessità di una terza parte che sia affidabile per validare le transazioni. Come vedremo è sufficiente il meccanismo del consenso per ottenere un accordo in merito alla validità delle transazioni.

Trasparenza e la fiducia. Poiché le blockchain sono condivise e chiunque può vederne i contenuti, questa caratteristica ne conferisce trasparenza e come conseguenza si stabilisce un livello di fiducia. (D'ora in poi: trust).

Immutabilità. Altro punto rilevante è costituito dall' immutabilità. Una volta scritti sulla blockchain, i dati sono praticamente immutabili. Di fatto è impossibile effettuare qualsiasi cambiamento senza che nessuno se ne accorga. Questa caratteristica conferisce alla blockchain il suo carattere di registro sicuro.

Disponibilità. Il sistema è organizzato in maniera tale da essere sempre disponibile anche se qualche nodo dovesse non esserlo.

Integrità. La crittografia asimmetrica conferisce sicurezza a ciascuna transazione assicurando l'integrità del network e rendendo di fatto sicura la blockchain.

Quanto sopra costituisce sicuramente un insieme di benefici "forti" riguardanti questa tecnologia. La loro importanza è indiscutibile e condivisibile in tutti gli ambiti nei quali si applica questo paradigma tecnologico.

Ci sono altri benefici che sono sicuramente importanti ma che potremmo indicare come aggiuntivi o "nice to have" soprattutto in certi ambienti tecnologici, e che la blockchain può assicurare.

Semplificazione dei paradigmi tecnologici. In situazioni nelle quali il modello dei dati è disorganizzato o disomogeneo, in cui entità multiple detengono i propri database rendendo complesso il loro mantenimento o la condivisione, l'adozione della tecnologia blockchain può comportare una semplificazione per il fatto che agisce come singolo registro dati suddiviso tra parti differenti.

Accordi più veloci. Nelle istituzioni finanziarie, specie durante le fasi di settlement successive a transazioni commerciali, la blockchain può giocare un ruolo fondamentale nella fase di settlement stesso; infatti la blockchain non necessita di un lungo processo di verifica, riconciliazione e di compensazione, poiché sul registro è già presente una versione dei dati che è già stata condivisa dalle varie parti e sulla quale c'è già stato un accordo.

Risparmio. Questo beneficio discende dal precedente. Non essendoci bisogno di infrastrutture dedicate a verifica, riconciliazione e compensazione di certe operazioni, i conseguenti costi e le fee pagate, cessano di esistere.

Infine, per completezza sembra corretto parlare anche dei limiti che attualmente sono introdotti da questa nuova tecnologia. Come in tutti i casi in cui sono adottati nuovi paradigmi tecnologici, è necessario operare alcuni correttivi affinché essi diventino più robusti, più utili e più accessibili.

Ad ogni modo i principali problemi di cui soffrono le blockchain sono:

- **scalabilità**
- **adattabilità**
- **regolamentazione**
- **tecnologia relativamente immatura.**

Ciascuno dei punti elencati presenta più che altro un problema principalmente tecnologico, pertanto la trattazione di ciascuno di essi, crediamo esuli dal presente articolo che vuole essere più divulgativo che tecnico.

In ogni caso esistono diversi approcci sotto esame mirati alla risoluzione anche di questi aspetti (si veda ad esempio https://doi.org/10.1007/978-3-662-53357-4_8 (acceduto il 15/02/2019) per uno dei possibili modi con cui rendere scalabile la blockchain).

4. Caratteristiche di una blockchain

Una blockchain implementa varie funzionalità che sono supportate da diverse caratteristiche:

Consenso distribuito. Il consenso è uno dei punti principali delle blockchain. Questo meccanismo consente alla blockchain di presentare un'unica versione della verità che è stata condivisa e sulla quale c'è dunque un accordo, da tutti gli attori, senza che vi sia necessità di un'autorità centrale atta a stabilirne la veridicità. Del consenso, e della sua enorme valenza, parleremo diffusamente tra breve.

Verifica delle transazioni. Ciascuna transazione inserita da un nodo sulla blockchain, è verificata sulla base di un insieme di regole predeterminate. Solo le transazioni valide sono selezionate per essere inserite in un blocco.

Piattaforma per Smart Contract. Una blockchain è una piattaforma sulla quale possono essere eseguiti programmi che automatizzano delle logiche di business nell'ambito di interesse degli utenti. Non tutte le blockchain possono eseguire smart contract, ma si tratta comunque di una funzionalità desiderabile e presente in tutte le ultime blockchain. Parleremo più diffusamente degli smart contract in un'apposita sezione.

Trasferimento di valore. La blockchain consente il trasferimento di valore tra utenti mediante l'utilizzo di token.

Creazione di criptovaluta. Questa caratteristica è opzionale e dipende dal tipo di blockchain utilizzata. E' comunque possibile per una blockchain creare criptovaluta la quale ha principalmente lo scopo di fungere da incentivo per i nodi che partecipano alla blockchain stessa, per ripagare il loro sforzo nel validare le transazioni e spendere risorse (macchina) per mantenere sicura la blockchain. Esiste poi anche l'a-

spetto speculativo relativo a questa funzionalità ma non è oggetto della nostra introduzione. Si parlerà in maggior dettaglio di criptovalute quando tratteremo il tema Bitcoin.

Smart property. E' possibile legare un asset fisico o digitale alla blockchain in modo sicuro e preciso e in maniera tale che la proprietà non possa essere rivendicata da alcun altro che non sia l'utente. L'utente è nel pieno controllo del proprio asset che non può essere speso due volte o posseduto due volte.

5. Tipologie di blockchain

La tecnologia della blockchain può essere suddivisa in diverse categorie, ciascuna con propri attributi, anche se in taluni casi questi sono sovrapponibili.

Da un punto di vista tecnico e di utilizzo possiamo citare:

- **DLT - Distributed Ledger Technology**
- **Blockchains**
- **Ledger**

Prima di descrivere le diverse tipologie è necessario un chiarimento terminologico. Con la locuzione "distributed ledger" (registri distribuiti), normalmente si fa riferimento ai database condivisi, da questo punto di vista, pertanto, qualsiasi blockchain ricade sotto la definizione di database o registro distribuito.

Sebbene quindi una blockchain è fondamentalmente un registro distribuito, non tutti i registri distribuiti sono classificabili come blockchain.

Una differenza fondamentale tra i registri distribuiti e le blockchain è che un registro distribuito non necessariamente consiste di blocchi di transazioni che aggiornano il database condiviso, ma le informazioni sono salvate in modo contiguo.

DLT

Soprattutto nel mondo della finanza, ultimamente, questo termine è utilizzato per descrivere la tecnologia blockchain. Spesso "blockchain" e "DLT" sono utilizzati in modo intercambiabile, e anche se ciò non è del tutto corretto, la recente evoluzione della terminologia ha portato a questa commistione di significati. Da un punto di vista finanziario i DLT sono blockchain permissioned (vedi oltre) che sono utilizzate e condivise tra utenti che si conoscono tra di loro. DLT vengono utilizzati come database condivisi che non generano una criptovaluta collegata nè hanno bisogno di un meccanismo per mettere in sicurezza il registro.

BLOCKCHAIN

La blockchain è costituita allo stesso tempo dal database e dal software che lo gestisce. Come software, la blockchain consente di caricare i dati direttamente nei vari nodi senza dover passare attraverso un nodo centrale al quale poi accedono gli altri. In questo senso la blockchain è un'applicazione peer-to-peer.

Esistono diverse sottocategorie:

- **Pubbliche:** *come suggerisce il nome non sono controllate da nessuno. Sono aperte al pubblico e chiunque può partecipare come nodo nel processo decisionale. Chi partecipa come nodo, viene chiamato "miner" (minatore). Il software della blockchain pubblica oltre a fare arrivare i dati a ciascun peer, si assicura e assicura a tutti i partecipanti, che i dati condivisi siano gli stessi. Questo processo è forzato. Se un dato cambia su un nodo, il cambiamento viene propagato a tutti i nodi. Infatti, tutti gli utenti di questi registri permissionless (cioè che non necessitano di un permesso per accedere, né i partecipanti devono essere noti) mantengono una copia del registro sul loro nodo locale e utilizzano un meccanismo di consenso distribuito per decidere l'eventuale nuovo stato del registro. Un esempio di blockchain pubblica è Bitcoin o Ethereum.*
- **Private (permissioned):** *come suggerisce il nome sono blockchain riservate tra gruppi di persone (consorzi, gruppi di individui o organizzazioni) che hanno deciso di condividere il registro tra loro. Come ovvio, una blockchain privata perde, in pratica, la caratteristica della decentralizzazione.*
- **Consortium blockchain:** *sono registri distribuiti dove il processo di consenso (relativo all'aggiunta dei dati) è controllato da un insieme preselezionato di nodi.*

Ai fini di quanto ci si prefigge in questa serie di articoli, non si reputa necessario indugiare ulteriormente con la tassonomia delle blockchain che è decisamente vasta e dotata di sfumature tecniche che necessitano di profonde conoscenze informatiche per essere comprese.

Passiamo pertanto a descrivere il meccanismo principale che costituisce assieme alla decentralizzazione, la spina dorsale della tecnologia blockchain: il consenso.

6. Consenso

Il consenso è, come detto, la spina dorsale della tecnologia blockchain, ed è quel meccanismo che consente di realizzare la decentralizzazione del controllo, attraverso un processo (opzionale) conosciuto con il termine inglese di "mining". La scelta dell'algoritmo di consenso è dipendente dal tipo di blockchain che si utilizza. Non tutti i meccanismi di consenso vanno bene per tutte le blockchain.

Il consenso è un processo per raggiungere un accordo (tra nodi o utenti che non si conoscono e che quindi non godono di trust reciproco), sullo stato finale dei dati che vengono "scolpiti" in un blocco in una determinata transazione.

Se da un lato è semplice raggiungere il consenso tra due nodi (si immagini ad esempio un rapporto client-server), quando i nodi sono molteplici, il raggiungimento del consenso su un singolo valore, diventa una sfida tecnologica importante. Il processo di ottenimento dell'accordo, sullo stato di una transazione, tra differenti nodi, è detto consenso distribuito.

Un algoritmo di consenso è costituito da una serie di regole che sono eseguite per step, dai nodi di una blockchain che intendono concordare su un valore o uno stato dei dati

condividendo.

Ciascun meccanismo di consenso è sviluppato per gestire le debolezze di un sistema distribuito e per consentire al medesimo sistema di ottenere uno stato finale di accordo.

Il consenso è un concetto ripreso dalla teoria del calcolo distribuito, che viene utilizzato in ambito blockchain, per avere un mezzo che consenta di trovare un accordo verso la stessa versione dei dati da parte di tutti i peer della blockchain.

Principali meccanismi di consenso

Traditional Byzantine Fault Tolerance (BFT)-based: composto di operazioni non complesse a livello di calcolo, il metodo ricalca uno schema in cui i nodi inviano messaggi firmati. L'accordo si raggiunge al ricevimento di un certo numero di "messaggi" firmati.

Leader election-based consensus mechanism: i nodi competono in una sorta di estrazione di un leader e il nodo vincitore propone il valore sul quale trovare l'accordo.

I due meccanismi rappresentati nel riquadro sono alternativi e performano in modo differente. Il BFT-based è adatto a situazioni nelle quali c'è un numero di nodi limitato e non scala molto bene; se ci si pensa, poiché devono essere scambiati molti messaggi prima di raggiungere un consenso, più nodi ci sono e più tempo ci vuole a raccogliere un numero di messaggi concordanti.

Il secondo meccanismo al contrario, scala molto bene ma è lento nell'esecuzione. Per inciso è il meccanismo nel quale ricade il proof of work (PoW) di Bitcoin. Questo è infatti il consenso utilizzato sulla blockchain della criptovaluta più famosa.

Esiste un grosso fermento relativamente la ricerca di meccanismi di consenso, che si prefiggono l'obiettivo di trovare il giusto bilanciamento tra scalabilità e performance, la loro descrizione però esula dal nostro perimetro.

Di seguito presentiamo una breve descrizione dei principali algoritmi di consenso disponibili oggi, partendo dal più famoso. Una selezione dei rimanenti sarà solo citata, per non dilungarci in tecnicismi che nulla aggiungerebbero al concetto generale già espresso: i meccanismi di consenso sono i più disparati dalle performance più diverse; la loro scelta dipende molto dal tipo di blockchain che si decide di utilizzare.

- Proof of Work(PoW): questo tipo di meccanismo per il consenso si basa sulla prova del fatto che da un nodo siano state consumate adeguate risorse computazionali, prima di presentare un valore all'accettazione del network (cioè prima di proporre la creazione di un nuovo blocco). E' il meccanismo adottato dalla blockchain di Bitcoin e di altre criptovalute. Per altro è l'unico che ha mostrato impenetrabilità da qualsiasi attacco hacker.

- Proof of Stake(PoS): questo tipo di algoritmo lavora sull'idea che un nodo abbia un livello di "coinvolgimento" (partecipazione) tale da rendere insensato da parte sua avere un comportamento malevolo. E' il consenso utilizzato sulla blockchain Ethereum. Nel consenso PoS, esiste anche il concetto di "coin age", che serve per tener conto, nella valutazione del nodo, del tempo e del numero di criptomonete detenute che non sono state spese.

- Delegated Proof of stake (DPoS): variazione del PoS. E' un algoritmo tramite il quale un nodo, sulla base del proprio stake (coinvolgimento), può votare per delegare un altro nodo ad effettuare la validazione della transazione.

Tra gli innumerevoli altri citiamo i seguenti meccanismi di consenso:

- Proof of Elapsed Time: meccanismo che mira a prevenire il consumo di risorse e tempo, utilizzando una sorta di lotteria per la scelta del nodo validatore

- Proof of Importance: l'algoritmo tiene conto non solo dello stake detenuto ma anche l'utilizzo e la movimentazione dei token, per stabilire un eleggibilità a nodo validatore.

- Proof of Deposit: basato sulla verifica che siano stati depositati fondi su un conto corrente bancario, prima di concedere ad un nodo la possibilità di validare transazioni.

- Proof of Activity: via di mezzo tra PoW e PoS.

A prescindere da quale sia il meccanismo di consenso scelto, ha rilevanza evidenziare che è sulla sua solidità e sulla sua efficacia che si basa la fiducia nelle transazioni validate su blockchain. Pertanto può preconfigurarsi una responsabilità degli ideatori e sviluppatori del meccanismo, nei confronti di chi utilizza il sistema. Nello stesso modo in cui chi realizza un software è responsabile nei confronti degli utenti terzi.

Nascono a questo punto temi di obsolescenza dell'algoritmo e di manutenibilità della blockchain connessa. E se si tiene presente che è proprio il meccanismo del consenso il punto sul quale si concentrano la maggior parte dei tentativi di attacchi malevoli alla resistenza della blockchain, ecco che diventa assolutamente importante, nel valutare scelte tecnologiche, il tipo di percorso che si intende effettuare per abbracciare tale tecnologia. Risulta pertanto evidente che una blockchain pubblica estesa, costituita cioè da una moltitudine di nodi, sarà più sicura rispetto ad una privata, la cui sicurezza è delegata alla sicurezza dei nodi che ne validano il relativo consenso.

Ci sia infine consentita una riflessione promossa principalmente da una sorta di "integralismo" tecnologico che analizza la questione solo dal punto di vista filosofico e non anche pratico: come detto altrove nella premessa, questa tecnologia a nostro avviso trova una delle sue ragioni d'essere, nella possibilità di consentire la decentralizzazione: dei dati e delle informazioni in generale. In un'epoca nella quale, chi detiene il dato, detiene anche un enorme "potere", ci sembra impreciso attribuire il "bollino" di soluzioni "innovative basate su blockchain", a soluzioni tecnologiche che non implichino l'utilizzo di una blockchain pubblica.

L'utilizzo di una blockchain privata (che come abbiamo detto è spesso un registro distribuito più che una blockchain vera e propria), proprio per come è intesa una blockchain privata, di fatto si concretizza nella realizzazione di un sistema "centralizzato". In questi casi il nostro consiglio è di non investire risorse econo-

miche in una blockchain o in un DLT ma, piuttosto, di dotarsi di un database. Motivazioni che spingono all'utilizzo di blockchain private, sono per lo più motivazioni di marketing. Ma questa è un'altra storia.

7. Decentralizzazione

Prima di affrontare l'ultimo punto (gli smart contract) di questa veloce panoramica sulla blockchain, e proprio per arrivare a parlarne, è interessante fare un approfondimento sulla decentralizzazione.

Come detto la decentralizzazione è la caratteristica principale che una tecnologia come questa si porta dietro e consente, in pratica, nel realizzare un'infrastruttura nella quale non c'è bisogno di un'autorità centrale.

Il controllo del paradigma, attraverso il meccanismo del consenso, viene consegnato agli utenti.

Dunque, da un punto di vista della blockchain, la decentralizzazione può essere vista come un meccanismo che fornisce un modo per rimodellare le tipologie di piattaforme esistenti o creare nuove applicazioni.

Convenzionalmente il mondo ITC, si è sempre basato su paradigmi centralizzati, dove i vari silos di dati o le diverse applicazioni sono sotto il controllo di un'autorità centrale che nella fattispecie viene chiamata Amministratore. Blockchain consente ora di realizzare sistemi decentralizzati ed operare senza che ci sia un punto singolo di possibile collasso o un'autorità centrale. Addirittura queste applicazioni possono funzionare autonomamente o su richiesta di un qualche intervento umano, a seconda di quale sia il modello di governance utilizzato nella applicazione decentralizzata che sta funzionando sulla blockchain.

Un sistema decentralizzato è un tipo di rete nella quale i nodi non dipendono da un singolo nodo mastro, ma il controllo è distribuito su vari nodi. Il consenso decentralizzato è poi la vera innovazione introdotta in questa nuova era di decentralizzazione delle applicazioni.

Possono essere utilizzati di fatto due metodi per realizzare la decentralizzazione:

- **disintermediazione**
- **competizione**

Con il primo metodo, di fatto, si va a "sottrarre" l'entità intermedia tra due parti che vogliono raggiungere un accordo. Tipo è l'esempio di trasferimento di denaro tra due persone: se avviene tramite l'intermediazione bancaria, esiste un'entità, (la banca) che si occupa del trasferimento del denaro e registra l'operazione su un registro centralizzato. Se tale passaggio avviene ad esempio su una blockchain, la necessità dell'intermediario viene meno essendo necessario solo l'indirizzo del borsellino elettronico del beneficiario.

Il metodo che comporta la competizione è meno "puro", e in sostanza è una modalità nella quale più offerenti un certo servizio, competono per essere quelli effettivamente designati ad offrirlo.

Il tema della decentralizzazione ci porta finalmente ad accennare ad uno dei concetti innovativi che sono stati introdotti con la blockchain Ethereum.

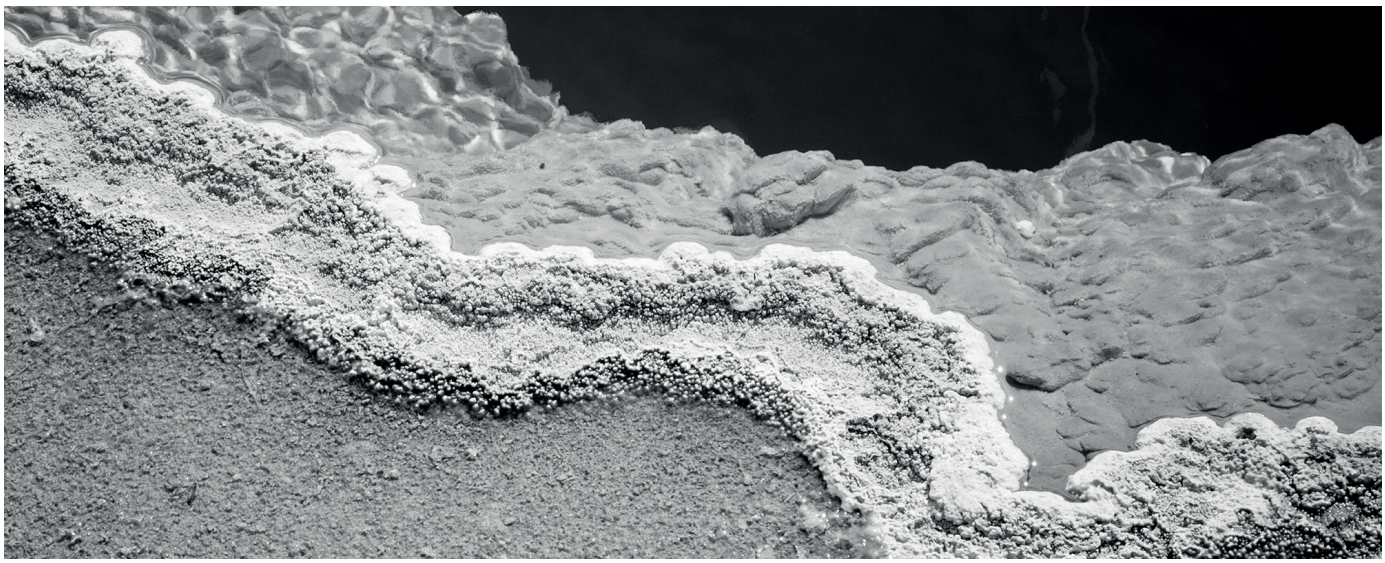
8. Smart contract

A dispetto del termine infelice, che fa sicuramente confusione in un contesto legale, gli smart contract sono, in realtà, programmi software decentralizzati.

Non è necessaria una blockchain per far eseguire uno smart contract, ma, in virtù dell'alto livello di sicurezza che la tecnologia blockchain garantisce, questa è diventata la piattaforma decentralizzata standard per l'esecuzione degli smart contract.

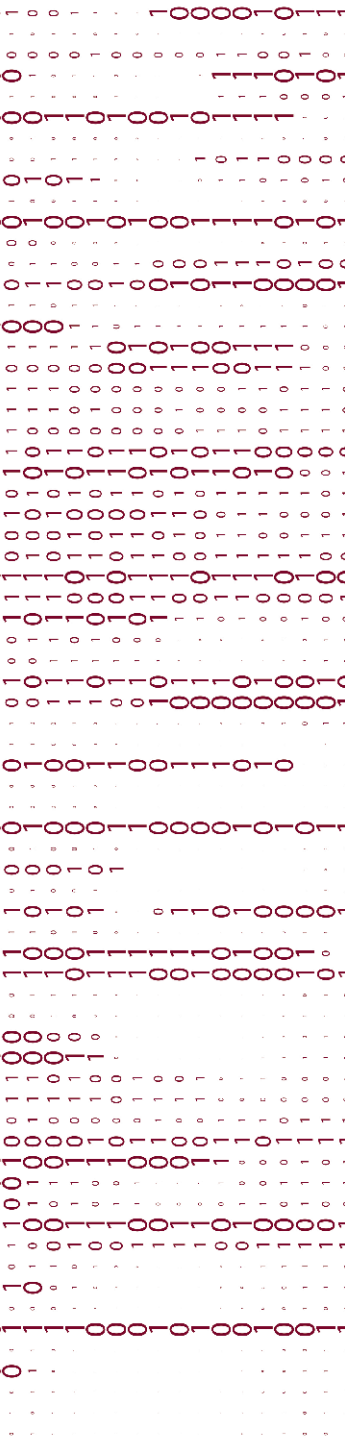
Di solito uno smart contract contiene della logica di business è un limitato ammontare di dati. La logica di business è eseguita se sono soddisfatti certi criteri specifici.

Luca Guiggi
Partner
Amministratore Delegato
www.omigrade.it



Blockchain in ambito legale e finanziario

Il caso www.lawonchain.io



Una delle proposte innovative nel vivace scenario tecnologico che ruota attorno alla tecnologia blockchain, è la piattaforma software LOC, acronimo di Law On Chain, che offrirà una serie di servizi con taglio prettamente rivolto al mondo legale e finanziario.

La particolarità della piattaforma è quella di appoggiarsi sulla tecnologia blockchain sfruttandone la decentralizzazione e la possibilità di automatizzare processi attraverso l'utilizzo di un linguaggio di scripting che consente di scrivere vero e proprio codice software che, rimappato ad esempio su una contrattualistica legale, consente di dare esecuzione, di fatto in modo automatico, ad un corrispondente insieme di parametri che possono essere descritti in un contratto legale.

L'esperienza di LOC offre l'occasione di illustrare come questa tecnologia si presti ad una serie di ambiti: TIMESTAMPING, FINANCIAL & BANKING SERVICES, COVENANT, RESTRUCTURING, ESCROW MANAGEMENT, M&A - SPA

TIMESTAMPING

Con il termine timestamping (tradotto in italiano con "notarizzazione", che però rischia di creare confusione richiamando la parola "notaio", ma che con l'ambito notarile non ha nulla a che fare), si intende la gestione di un dato o di una serie di dati, attraverso una cristallizzazione di essi o di una loro parte rappresentativa, in un blocco della blockchain.

In linea generale, un registro, è uno strumento utilizzato "per avvicinarsi alla verità" o per raggiungere "un'approssimazione alla verità" che sia accettabile da tutti gli interessati.

La situazione ideale si ha quando i registri non sono controllati da nessuno in particolare, ma sono disponibili a tutti e da tutti sono verificabili.

In questo senso si può dare la possibilità di fissare in modo indelebile un "fatto" (dato), affinché questo non sia né modificabile né cancellabile ma resti sempre a disposizione di chiunque voglia verificarlo o controllarlo.

Una funzionalità di timestamping consente di fare proprio questo. Cristallizzare in un luogo pubblico (inteso come luogo non centralizzato, cioè non sotto il controllo di un'entità che lo amministra), un'informazione o una sua rappresentazione fedele, perché da lei ricavata (hash).

Il timestamping è equiparabile ad una firma digitale (o ad una pec), e consente di ricavare anche un'impronta digitale dei dati oggetto del trattamento.

Il dati possono anche essere criptati per rispettare normative di privacy, qualora questa cosa fosse necessaria. I contenuti poi possono essere resi in chiaro chi ha i diritti di visualizzazione.

FINANCIAL AND BANKING SERVICES

Questo tipo di funzionalità consentono di automatizzare una serie di attività normalmente curate da un c.d. agente mandatario, in ambito di accordi di finanziamento (controllo di Covenant), e ristrutturazione finanziaria (Restructuring).

Questa funzionalità può essere a supporto di tutti quei professionisti che operano nei processi di back&middle office in operazioni finanziarie e di controllo dei workflow operativi.

In questo senso è possibile operare un controllo dei financial covenants che regolano un contratto di finanziamento, seguendo le scadenze previste dagli accordi.

Una volta impostato il contratto e sistemate le relative clausole, lo smart contract riceverà un ok/ko sulla base di verifiche fatte dal contract manager (figura inizialmente umana ma in prospettiva sostituibile da un apposito strato software), ed esegue o meno certe azioni previste dall'accordo legale originario.

Attraverso una parametrizzazione appropriata, è possibile abbracciare il più ampio numero di casi possibili, nell'ottica di offrire il massimo livello di automazione, realizzando quindi uno scenario rappresentabile come una vera e propria DAPP. (Applicazione distribuita).

Per quanto riguarda le "operazioni di restructuring", con questo termine indichiamo tutte quelle operazioni volte alla risoluzione di crisi aziendali causate dalle più disparate ragioni, endogene o esogene. Comunemente, con il termine "restructuring" si indicano tutte quelle operazioni di natura straordinaria preordinate a riportare un pareggio di bilancio, là ove non c'era, identificando i fabbisogni, pianificando le azioni per riportare a redditività l'attività aziendale. L'attività di restructuring è dunque un'operazione complessa che dev'essere impostata con un approccio multidisciplinare poiché una ristrutturazione del debito ha successo solo se accompagnata dalle giuste scelte strategiche e dall'implementazione delle corrette politiche aziendali.

In tale percorso, è evidente che l'accordo con i principali creditori rivesta il principale ruolo. Che si tratti di un accordo extragiudiziale, che si tratti di un c.d. piano attestato o che si tratti di una ristrutturazione ex art. 182 bis L.F., l'accordo con le banche ha spesso caratteristiche comuni su cui è possibile intervenire con un servizio effettivamente innovativo.

Infatti una delle feature offerte da una soluzione basata su blockchain è in effetti quella di automatizzare l'attività di monitoring dell'impresa, conseguente all'adozione degli accordi di risanamento, andando a sostituire l'attività sino ad oggi svolta dal già citato "agente", in particolar modo sul rispetto da parte della debitrice dei parametri finanziari. Tale attività si concretizza pertanto nella verifica del rispetto del programma di risanamento e nel fornire una visualizzazione immediata dell'adempimento della debitrice rispetto a tutti gli adempimenti richiesti dagli accordi intercorsi.

Proprio per facilitare queste attività di controllo, è possibile fornire uno strumento con il quale automatizzare tali compiti di verifica demandandoli ad esecuzioni a carico di smart contract che vengono eseguiti su una blockchain, con la possibilità di registrare di volta in volta l'iter seguito e registrando con il timestamping l'esecuzione delle varie operazioni. (si veda sopra il paragrafo sulla funzione di timestamping).

ESCROW MANAGEMENT

Si tratta del servizio di gestione delle garanzie che possono nascere o come contratti a sé stanti o da uno degli accordi citati in precedenza o, ancora, come attività integrativa necessaria al completamento di un iter di acquisizione regolato tramite contratto M&A (nella fattispecie che ci riguarda SPA) di cui si parlerà oltre.

Vediamo un esempio di come mappare un contratto di garanzia tra due parti.

Un contratto di escrow è un accordo tra tre parti, in cui una parte (Contract Manager) detiene e regola il pagamento dei fondi che deve avvenire tra le altre due parti (in genere un acquirente e un venditore). Ad esempio un tale tipo di contratto può essere utilizzato da un acquirente e venditore per rendere più sicura la loro transazione. Il pagamento o parte di esso, viene tenuto in un conto sicuro e rilasciato quando tutti i termini del contratto sono soddisfatti.

L'acquirente attiva uno smart contract per gestire la garanzia e effettua un deposito di tale garanzia. Durante l'inizializzazione del contratto, l'acquirente fornisce l'indirizzo del venditore, un tempo di scadenza del contratto e un valore.

Il contratto di garanzia è distribuito su una blockchain, (ad esempio ETHEREUM) e il deposito è detenuto nel conto del contratto o su un conto bancario in caso di moneta fiat. Il venditore quindi esegue il servizio per l'acquirente e quest'ultimo controlla il servizio consegnato. Con la ricezione della documentazione contrattuale o comunque dopo le verifiche, l'importo dell'anticipo verrà rilasciato anche i modo automatico al venditore.

M&A (SPA)

Con la locuzione operazioni di M&A, nella prassi si individuano tutte quelle operazioni di natura straordinaria volte sostanzialmente alla concentrazione nelle mani di un unico soggetto economico della proprietà delle attività aziendali di un altro soggetto economico, nonché tutte le attività ancillari volte al conseguimento di tale concentrazione. In particolare, l'integrazione di due o più imprese può avvenire secondo molteplici forme, consensuali o ostili, avendo quale oggetto immediato le aziende e dunque i beni attraverso cui viene svolta l'attività d'impresa (ed in questo caso si parla di asset deals) ovvero le partecipazioni nel capitale sociale delle società che detengono tali aziende (ed in questo caso si parlerà di share deals). Tra gli share deals, poi le strutture contrattuali possibili sono sostanzialmente infinite, adattabili ad ogni specifica circostanza concreta e, tuttavia, in estrema sintesi si possono individuare operazioni di fusione, ove due o più società che abbiano business integrabili, si uniscono a formare una unitaria realtà aziendale e societaria, ovvero acquisizioni ove un soggetto acquisti parte o tutte le partecipazioni al capitale sociale di altro soggetto economico.

Anche in questo caso, il panorama di possibili transazioni prevede innumerevoli strutture negoziali complesse e collegate, spesso molto diverse tra loro ove, tuttavia, vi sono talune significative caratteristiche comuni che la comunità legale internazionale ha tipizzato nel cosiddetto Share Purchase Agreement e nei contratti di finanziamento che la c.d. BidCo, ovvero l'acquirente, stipula con il sistema bancario onde ottenere la (o parte della) provvista necessaria all'acquisto. Contratti complessi, adeguati alle diverse giurisdizioni nelle quali essi sono chiamati ad essere applicati e tuttavia –come detto- con caratteristiche e clausole comuni.

Un contratto SPA, come più sopra abbiamo visto, regolamenta -inter alios- l'acquisto e la vendita, tra due o più parti, delle partecipazioni di una società target. I termini di tale operazione, sono descritti in modo dettagliato e l'intera operazione d'acquisto è soggetta al rispetto di specifiche modalità esecutive o ad eventuali condizioni sospensive o risolutive. Il Venditore poi concede specifiche garanzie e si impegna ad indennizzare dettagliati eventi futuri idonei a causare pregiudizio all'acquirente.

In quest'ultimo scenario poi si innesta il tema dell'escrow management, già trattato in un apposito paragrafo.

Luca Guiggi
(www.omigrade.it)

Il nuovo accesso al credito mediante tecnologia Blockchain

ICO e CICO

Uno degli argomenti più controversi nonché uno degli acronimi più ricorrenti su Google a cavallo tra l'anno 2017 e il 2018 è sicuramente la parola Ico ovvero "initial coin offering".

Una breve analisi condotta direttamente sulla tendenza delle ricerche a livello globale, fa emergere che il termine Ico è secondo solo alla parola Bitcoin.

Ma cosa è una Ico? A cosa serve? Cosa c'entra con la blockchain? E perché tutti la associano alle criptovalute?

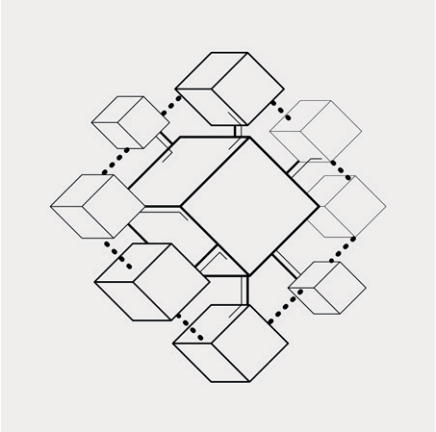
Partiamo dal principio.

L' Ico altri non è che uno strumento, speculare all' offerta pubblica iniziale di azioni nei mercati finanziari, che a differenza di essere emessa da società ben solide e strutturate, viene impiegata, nella maggior parte dei casi, da acerbe start-ups che aspirano a raccogliere fondi da stanziare per il finanziamento del proprio progetto.

Scopo precipuo di una Ico è, tout court, la raccolta di capitale, il quale, verrà impiegato dal team della neonata società per sviluppare il progetto nel quale, gli investitori, hanno riposto fede basandosi esclusivamente su un piano progettuale: il "white paper".

Quest'ultimo è l'unico documento dal quale è possibile attingere tutte le informazioni per valutare la bontà del progetto. Volendo spingersi oltre, una Ico, si potrebbe definire come un metodo di finanziamento bottom–up e che assume i connotati del "reward-crowdfunding".

Il meccanismo retrostante è piuttosto semplice: la start up, a fronte dell'entità di un versamento corrispostole, restituisce agli investitori dei token (gettoni) i quali oltre a simboleggiare il coinvolgimento nel progetto stesso, hanno anche un valore intrinseco attribuitogli in base alla token economics (studi economici retrostanti la struttura



di un token).

Per chiarire l'inscindibile nesso tra blockchain e Ico, immaginiamo che tra i due vi sia un rapporto di genus a species, dove il primo è l'infrastruttura tecnologica di base, con regole e funzionamenti propri che, favorendo e semplificando il lavoro di raccolta e gestione trasparente dei fondi, funge da mezzo per il trasferimento di "valore" tra i soggetti che prendono parte a questo scambio. Volendo passare ad aspetti leggermente più tecnici -per approfondire e voler dare risposta ai quesiti summenzionati, senza voler peccare di presunzione nell'esaustività dell'argomento- è giocoforza chiarire l'oggetto di una Ico.

Ora, per correttezza d'esposizione, è bene precisare che il token emesso dalla società, avrà, secondo la più recente dottrina, natura legale assimilabile a quella di un coupon o gift card da spendere all'interno della piattaforma creata ad hoc dal team.

E' proprio dalla sua funzione/natura che prende il nome di "utility token", poiché è necessario possedere quel token per poter fruire di un determinato servizio o comprare un determinato bene all'interno dell'ecosistema appositamente creato.

Oltre agli utility si è soliti annoverare altre due macro categorie di token con inquadramenti (legali, fiscali, tecnici) differenti dai primi:

1) i securities
2) i payments.

Per quanto riguarda i primi, questi sono generalmente equiparati a titoli veri e propri che possono essere equiparati a quote, dividendi, azioni e obbligazioni in base alle volontà dell'emittente. Proprio come gli strumenti finanziari essi devono rispettare determinati criteri imposti da normative come la Mifid 2 piuttosto che la Mifir, il nuovo regolamento europeo sulla protezione dei dati, disposizioni in ambito bancario, di diritto commerciale internazionale nonché di diritto fallimentare. Nel caso in cui si intendesse emettere un security token, ad onor del vero, si starebbe portando avanti una STO (security token offering) assoggettandosi in tutto e per tutto alle stesse norme di chi si cimenta nel lancio di una IPO.

In questo caso la due diligence e la compliance aziendale diventano fattori di estrema importanza al fine di evitare pesanti ripercussioni sia in termini di sanzioni che in ambito di business nei confronti degli investitori. A tal proposito merita un accenno il fatto che la SEC (Securities and Exchange Commission) ente statunitense preposto alla vigilanza della borsa valori, abbia iniziato un un bel giro di vite nei confronti di quelle società che, avvalendosi della precedente lacuna normativa, abbiano emesso security spacciandole per utility. Tutto ciò portando ovviamente ad un importante risparmio in termini fiscali e legali, e non garantendo quella protezione all'investitore tipica dei titoli, in quanto, come ben saprete, la gestione di un titolo è una spesa completamente differente da sostenere rispetto al costo necessario per poter vendere un bene o prestare un servizio.

Per quel che riguarda i payment token, questi vengono identificati come mezzi di scambio alternativi alle valute, utilizzabili per pagare beni e/o servizi. Caratteristiche principali di questo tipo di token è che non sono emessi ne sostenuti da un ente centrale ne da una banca, circolano su piattaforme "distributed ledger" e sono identificati come "token nativi" ovvero sono dotati di una propria piattaforma e un proprio protocollo applicativo.

Gli esempi più ricorrenti di payment token sono le criptomonete: Bitcoin, Ethereum e Litecoin. Volendo solo in questo caso, peccare di pignoleria, definire Bitcoin, Ethereum e Litecoin come token è considerato un errore dai più radicali in quanto si è soliti fare una distinzione tra coin e token.

La differenza sostanziale risiede nel fatto che le coin non si appoggiano ad una blockchain ospite ma ne possiedono una propria con il proprio algoritmo di consenso, propri standard e protocolli. Dopo aver tracciato una panoramica sul funzionamento, sullo scopo, sull'oggetto e sul sommario inquadramento giuridico, mi premeva spendere due righe su un aspetto che raramente riesce ad emergere nelle trattazioni di stampo scientifico e che si colloca nelle retrovie rispetto all'organizzazione, la gestione e la promozione di una Ico.

Uno degli elementi più importanti in fase di valutazione, ricade sicuramente sui membri del team. Mai come in questi casi l'unione fa la forza; senza coesione, passione e visione prospettica d'insieme, nessun piano progettuale è destinato a prosperare.

Senza essere prolisso ritengo che le competenze necessarie all'interno dell'organico dovranno spaziare dall'ambito di sviluppo software/hardware al campo economico passando per quello legale senza tralasciare quello di marketing e branding digitale.

Un altro aspetto fondamentale che ho riscoperto attraverso le varie consulenze, la lettura d'innumerevoli libri, articoli e interviste è che la collaborazione è la chiave del successo. Un concetto questo che sembra esulare dal contesto fin-tech ma che, se ci si guarda attorno, sta avendo luogo anche in

ambienti del tutto estranei all'oggetto di questa trattazione. Le varie fusioni, acquisizioni, consorzi in ambito alimentare/automotive/oil & gas sono un esempio di lapalissiana evidenza di come la società stia cambiando per far fronte alle nuove sfide che ogni giorno ci si trova ad affrontare, bisogna allearsi. Il mondo del lavoro è in continua evoluzione se poi si pensa al settore tecnologico degli ultimi trent'anni ci si può rendere davvero conto di come sia indispensabile strutturare degli organismi dotati di personale multi competente e multitasking per poter stare al passo.

Allo stesso modo si potrà sicuramente scusare il legislatore che puntualmente si trova a "pezzare normativamente" le fattispecie che si vengono a creare grazie all'impatto che hanno le evoluzioni tecnologiche sulle nostre vite. Ed è proprio tornando sull'aspetto legislativo della questione che si sta giocando la battaglia più importante. In questo periodo, il Ministero dello sviluppo economico, dopo avere reclutato i 30 esperti in materia di blockchain, sta cercando di creare ex novo un quadro normativo in grado di regolare questa nuova tecnologia e i suoi casi d'uso. Inutile dire che un'armonizzazione almeno a livello europeo sarebbe fortemente gradita, specialmente per gli operatori dei servizi connessi al lancio di una Ico, che attualmente trovano diversi ostacoli nel doversi relazionare con realtà del tutto estranee e alquanto diverse dalla nostrana.

Giungendo a conclusione mi sembra opportuno menzionare il fatto che il boom delle Ico risalente al 2017 rimane un lontano ricordo sia in quanto ai numeri raggiunti (si pensi ai 6,2 miliardi di dollari raccolti nello stesso anno), sia per ciò che riguarda l'impostazione giuridica della maggior parte delle start-ups, scevra da qualsiasi indirizzo di compliance.

Grazie alla tecnologia blockchain, a mio avviso, i legali più pionieristici potranno aprirsi nuovi canali di business ancora inesplorati che prima per ovvie ragioni gli erano preclusi.

Molti attori coinvolti nel mercato delle criptomonete brancolano nel buio dell' incertezza non avendo ben chiaro se: possano vantare diritti e di che natura, se possono godere di una qualche tutela, che rischi corrono a intraprendere certe azioni e che ripercussioni possono avere sulla loro persona/patrimonio; per non parlare di tutti gli aspetti fiscali correlati alla compravendita di token, alla speculazione ,alla custodia e all' utilizzo di exchange decentralizzati o sistemi over the counter (otc), solo per citarne alcuni.

La platea di possibili clienti aumenta esponenzialmente di mese in mese sia tra le persone fisiche che tra le persone giuridiche. Il fatto è che per poter soddisfare una domanda cosi importante bisogna che l'offerta sia altamente qualificata e competente almeno nel campo tecnologico e finanziario, oltre che legale si intende.

Di qui, riprendo l'importanza del discorso sulla collaborazione e sul dotarsi di persone che abbiano attitudini e competenze diverse ma complementari e che abbiano una visione condivisa dello stesso obiettivo. La tecnologia blockchain dovrebbe essere intesa come una sorta di nostra alleata, uno strumento che semplifica, velocizza e riduce i costi di determinate fasi lavorative; non di certo bisogna demonizzarla come un qualcosa che sottrae lavoro o peggio ancora ci rimpiazza del tutto. Senza di essa sarebbe un po' come tornare indietro e continuare a scrivere a macchina anziché utilizzare l'ausilio del pc e del programma word, sicuramente più affascinante e romantico ma insostenibile a livello produttivo, considerando poi il carico di lavoro a cui sono sottoposti gli studi legali odierni. Forse il paragone è un po' estremizzato ma il mio intento è proprio quello di suscitare un frammento di curiosità per questo tema, portando a galla una riflessione che adesso lascio approfondire a voi.

Giannandrea Garau
Legal Advisor di Cripton.it

Breve schema riassuntivo

STO (security token offering)

1. Conforme alle norme sui titoli
2. Basso profilo di rischio
3. Supportata da beni come collaterale
4. Facile valutazione del vero valore

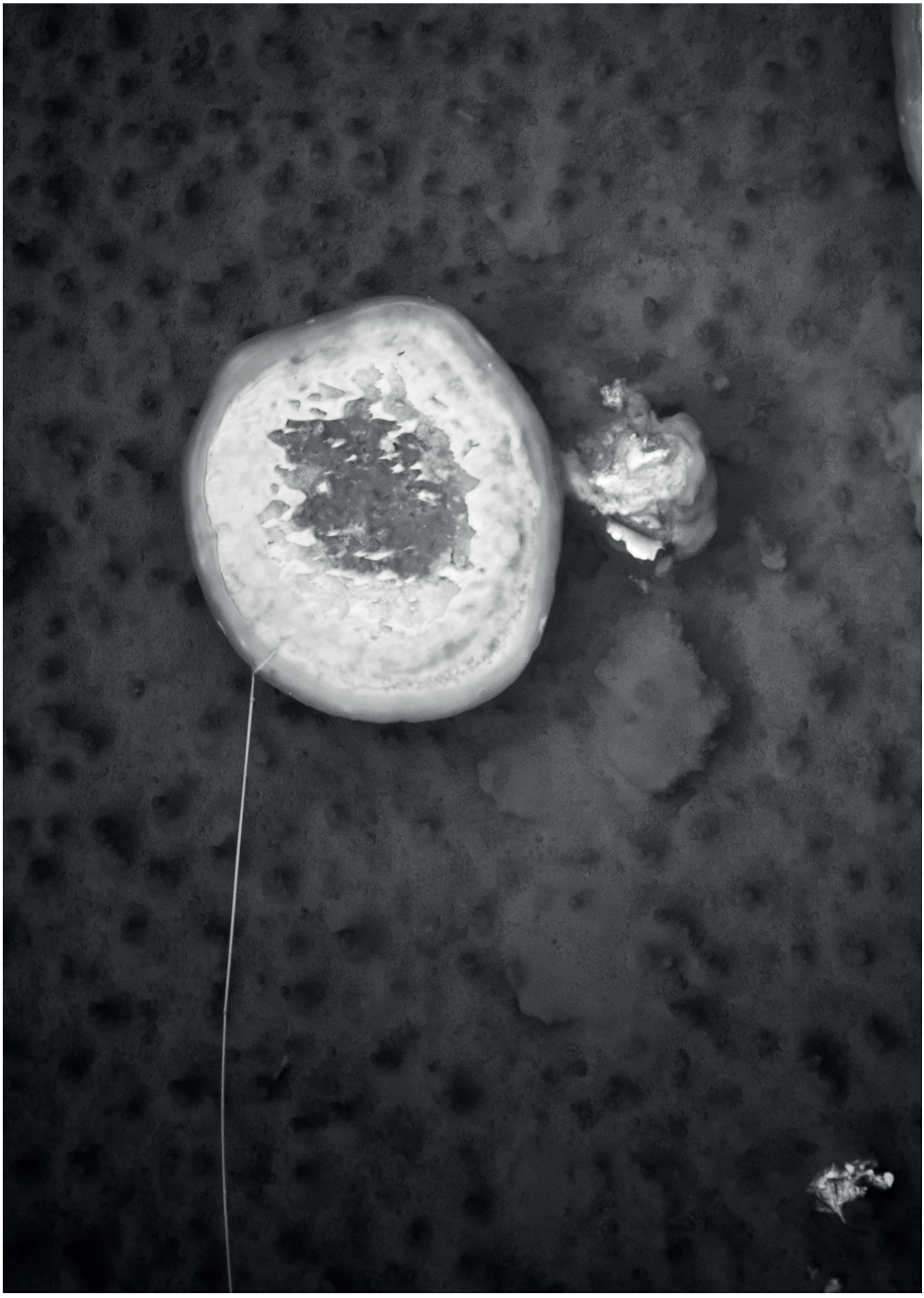
VS

ICO (initial coin offering)

1. Non vi sono requisiti da rispettare
2. Alto rischio per gli investitori
3. Non vi è un collaterale sottostante
4. Vero valore difficilmente valutabile

IPO (initial public offering)

1. Dipendenza totale da intermediari finanziari (banche, broker, ecc.)
2. Tasse di quotazione molto alte
3. Compravendita limitata alle azioni della società
4. Poca liquidità



Smart contracts

Gli smart contracts non sono altro che dei contratti "tradizionali" che vengono trasposti in un codice software (un algoritmo) in grado di verificare in modo automatizzato l'avverarsi di determinate condizioni concordate tra le parti dandone automatica esecuzione.

Il codice software interviene quindi nella fase di esecuzione del contratto e applica automaticamente le clausole pattuite nel momento in cui si verificano determinati avvenimenti specificati nel contratto medesimo.

In sintesi, gli smart contracts sono quindi contratti tradizionali tradotti in un programma software che ne automatizza l'esecuzione.

Formule basiche di smart contracts sono state oggetto di sperimentazione fin dagli anni '90.

All'epoca l'esigenza era quella di gestire in automatico, tramite una chiave digitale, l'attivazione e/o disattivazione di una licenza software al verificarsi di alcune condizioni quali il pagamento della licenza stessa e la data di scadenza del contratto.

Le chiavi digitali utilizzate non davano però garanzie di sicurezza, immutabilità e trasparenza.

E si tratta di caratteristiche fondamentali per lo sviluppo e l'utilizzo degli smart contracts che, quali contratti dematerializzati e presenti sulla rete, devono appunto garantire che il codice con cui sono stati scritti non sia modificabile da una delle parti, che le fonti di dati che determinano le condizioni di applicazione e le modalità di lettura e controllo di queste fonti siano certificate ed affidabili.

A dette problematiche ha dato un risposta il protocollo blockchain che ha avuto uno sviluppo incredibile grazie al fenomeno bitcoin.

La blockchain, di cui si è già parlato negli articoli che precedono, è anche definita come l'internet dei contratti.

Si tratta di un sistema decentralizzato e aperto, senza alcun proprietario ed utilizzabile da tutti, i cui dati non possono essere modificati o meglio, possono essere modificati solo aggiungendo altre righe di codice.

E visto che ogni operazione su blockchain è permanente, ogni modifica è registrata e visibile da tutti. E' quindi impossibile apportare modifiche senza che tutti se ne accorgano.

Per tale ragione l'art. 8 comma 2 del Dl 135/2018(decreto semplificazioni) definisce gli smart contracts come *"un programma per elaboratore che opera su tecnologie basate su registri condivisi e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse."*

Il nostro legislatore ha quindi individuato come piattaforma affidabile la tecnologia blockchain e cioè i registri distribuiti proprio perché garantiscono la sicurezza, la trasparenza e l'immutabilità degli smart contracts.

Detta norma ha sollevato qualche perplessità, in particolare con riferimento al fatto che si parli solo di esecuzione(vincolante) del contratto sulla base di effetti predefiniti dalle parti, e non di formazione del consenso, di obblighi informativi a favore del contraente debole e di rimedi anche giudiziali esperibili in caso di inadempimento e/o di altre patologie contrattuali.

Seguendo la definizione data dal nostro legislatore, sembrerebbe quindi che gli smart contracts non possano essere considerati dei veri e propri contratti in quanto non sono scritti in un linguaggio standard, ma bensì in un linguaggio informatico (*"programmi per elaboratore"* e cioè dei software) ed, in secondo luogo, perché possono sostituire solo la fase esecutiva di un contratto, automatizzandola, ma non la parte descrittiva con le relative pattuizione.

Ora, per ulteriori commenti, sarà necessario attendere le Linee Guida che l'Agenzia per l'Italia Digitale dovrà emanare nei prossimi mesi.

Resta comunque il fatto che per dare esecuzione ad un contratto è perlomeno necessario che ci sia una fonte contrattuale condivisa tra le parti e perciò almeno scritta in un linguaggio che sia comprensibile da entrambe.

Lo smart contract dovrebbe quindi nascere come documento *"standard"* intellegibile da entrambe le parti che dovrà poi essere trasformato in codice software e caricato sulla piattaforma blockchain ai fini della sua automatica esecuzione.

Attendiamo comunque le Linee Guida per ulteriori commenti.

La seconda parte del 2° comma dell'art. 8 ter dispone che *"gli smart contracts soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia pere l'Italia digitale con le linee guida da adottare entro 90 giorni dalla entrata in vigore della legge di conversione del presente decreto".*

Il decreto è stato convertito dalla Legge n. 12/2019 che è entrata in vigore il 13 febbraio 2019.

Ad oggi le linee guida non sono ancora state adottate.

Detta norma, secondo alcuni autori, risulta superflua visto che gli smart contracts costituiscono già un documento informatico, e cioè un documento che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, che ai sensi dell'art. 20 comma 1 bis del

Codice dell'Amministrazione Digitale (Dlgs 82/2005) *"soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'art. 2702 c.c. quando"* ha determinate caratteristiche.

Lacunosa perché il Decreto Semplificazioni non indica le modalità con cui gli smart contracts, oltre alla forma scritta, potranno essere ricondotti nell'alveo delle scritture private di cui all'art. 2702 c.c. con il relativo valore probatorio.

Chi vivrà vedrà. Sta di fatto che la questione, che potrebbe forse annoverarsi nell'alveo di quelle inutili, si sarebbe potuta risolvere a priori semplicemente aggiungendo una riga all'articolo o, magari, semplicemente definendo gli smart contracts come documenti informatici ai sensi del Codice dell'Amministrazione Digitale.

Il 3 comma dell'art. 8 ter stabilisce poi che "la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti della validazione temporale elettronica di cui all'art. 41 del Regolamento UE n. 910/2014 del 23 luglio 2014 (Regolamento e-IDAS).

Per validazione temporale elettronica, ai sensi del Regolamento e.IDAS, si intende il collegamento "dei dati in forma elettronica ad una particolare data e ora, così da provare che questi ultimi esistevano in quel momento".

Anche in questo caso, per conoscere gli standard tecnici che le tecnologie basate su registri distribuiti debbano possedere per produrre gli effetti di cui al comma 3, bisognerà attendere le Linee guida che l'Agenzia per l'Italia Digitale dovrà predisporre entro 90 giorni decorrenti dal 13 febbraio 2019.

Gli smart contracts stanno suscitando molto interesse soprattutto nel mondo assicurativo, bancario, finanziario ed immobiliare.

L'interesse è dovuto al fatto che grazie alla tecnologia blockchain non vi è la necessità di intermediari (riducendo così i costi), è garantita la sicurezza e l'immutabilità ed, infine, vengono evitati gli errori, essendo la fase esecutiva totalmente automatizzata.

Un primo esempio di smart contract arriva dal mondo assicurativo ed in particolare dalle nuove formule di rc auto che prevedono l'installazione di un dispositivo "Internet of Things" a bordo del veicolo.

Detti dispositivi connessi ad internet sono in grado di fornire dati sul comportamento del conducente che possono attivare automaticamente clausole contrattuali vantaggiose o svantaggiose. Se per esempio vengono superati i limiti di velocità contrattualmente pattuiti in automatico il contratto applicherà quelle clausole che prevedono un aumento del premio assicurativo prelevando direttamente dal c/c o dalla carta di credito dell'assicurato quanto dovuto.

Un altro esempio riguarda il diritto d'autore e l'accesso ai servizi multimediali on line, dove la possibilità di scaricare un libro o un film o ascoltare musica viene gestito in automatico, e cioè senza intervento umano, da uno smart contract che, previa verifica del servizio acquistato e delle condizioni contrattuali pattuite al momento dell'iscrizione ad una piattaforma, ci permette o meno l'accesso al servizio richiesto.

Come abbiamo già detto, altro settore particolarmente interessato agli smart contracts è quello immobiliare e cioè compravendite ed affitti.

Un esempio ci arriva dalla Svezia, dove il catasto ha siglato un accordo con una start up per creare un protocollo per l'utilizzo degli smart contracts e della blockchain per le compravendite immobiliari.

Detto sistema è attualmente inutilizzabile, o meglio, utilizzabile in modo assai depotenziato, nel nostro Paese vista la normativa in vigore. Se però facessi il notaio inizierei a preoccuparmi.

A questo punto, direi che è giunto il momento per un paio di riflessioni finali.

La prima riguarda l'incompletezza e fumosità della normativa che abbiamo analizzato che lascia parecchie perplessità. Ci auguriamo quindi che le Linee Guida che verranno approvate dall'Agenzia per l'Italia Digitale facciano un po' di chiarezza.

Al di là di questo, gli smart contracts e la blockchain saranno probabilmente il futuro della contrattualistica su larga scala.

E se così sarà, si porranno inevitabilmente delle problematiche in materia di privacy, visto che la diffusione di tali contratti porterà sulla blockchain, che è un sistema aperto in cui tutti possono vedere tutto, una montagna di dati personali.

Si dovrà quindi inevitabilmente intervenire con una normativa specifica a tutela della privacy, anche in considerazione del fatto che il grande business del presente e del futuro è proprio quello della raccolta e della gestione di detti dati a fini commerciali.

L'ultima riflessione riguarda invece il ruolo dell'avvocato in questo settore.

L'automazione e l'informatizzazione, che sta cambiando radicalmente e molto velocemente il settore industriale, sta di fatto entrando in fretta anche nel settore dei servizi, inclusi quelli legali.

Già il settore degli smart contracts richiederà agli avvocati qualche nozione informatica in più di quelle scarne conoscenze che abbiamo ora e ci imporrà di lavorare fianco a fianco con uno sviluppatore informatico.

L'avvocato si occuperà della redazione del contratto, lo sviluppatore della sua "traduzione" in codice software.

Ma sarà davvero così?

Già esistono robot, dotati di intelligenza artificiale, che in pochi minuti riescono a redigere un documento legale che ad un avvocato umano richiederebbe qualche ora (uno di questi si chiama MarginMatrix).

E se consideriamo che smart contracts e blockchain hanno, tra i loro "vantaggi", proprio quello di ridurre i costi eliminando gli intermediari, e cioè i professionisti, credo che il rischio che questo settore ci sfugga di mano sia elevato.

Pietro Pettenati

SPID

Lo SPID, il Sistema Pubblico di Identità Digitale, è presentato come la soluzione che permette di accedere a tutti i servizi on-line della Pubblica Amministrazione con una sola identità digitale (combinazione di una username ed una password) utilizzabile su qualsiasi computer, tablet e smartphone.

Per attivare lo SPID è necessario avere un indirizzo e-mail, un telefono cellulare, un documento di identità valido e la tessera sanitaria riportante il codice fiscale.

La registrazione si completa con il riconoscimento personale (ovvero incontrando un incaricato che possa identificare l'utente) oppure anche con altre modalità, variabili a seconda dell'ente certificatore scelto: con le modalità diverse da quella dell'incontro fisico può essere chiesto un pagamento per il servizio.

Ricevuta la conferma della registrazione sarà possibile utilizzare tutti i servizi informatici della pubblica amministrazione con un'unica identità elettronica e, quindi, senza avere registrazioni specifiche per ogni servizio.

A partire dal 9 aprile 2018 l'area riservata dell'Agenzia Entrate è accessibile agli utenti persone fisiche anche tramite la propria identità digitale SPID - livello 2.

L'accesso all'area riservata da parte dei soggetti diversi dalle persone fisiche avviene per il tramite degli incaricati, l'identità digitale in tal caso, si intende riferita a questi ultimi.

A stabilirlo è il Provvedimento del 9 aprile 2018 n. 75242.[1]

1 Ad oggi sul sito SPID c'è il riferimento ai seguenti servizi accessibili.
Agricoltura, pesca, silvicoltura e prodotti alimentari (Finanziamenti Iscrizione a servizi Servizi INAIL)
Ambiente (Edilizia Portali del cittadino Servizi INAIL Servizi di pagamento, controllo pagamenti, tasse e tributi Visure, controllo e consultazione dati)
Economia e finanze (Anagrafe Fatturazione elettronica Finanziamenti Invio e richiesta documenti Richieste e prenotazioni Servizi INAIL Servizi INPS Servizi di Certificazione e Autocertificazione Servizi di pagamento, controllo pagamenti, tasse e tributi Utilità Tutte le categorie per Economia e finanze)
Giustizia, sistema giuridico e sicurezza pubblica (Servizi INPS Utilità)
Governo e settore pubblico (Anagrafe Edilizia Finanziamenti Invio e richiesta documenti Iscrizione a servizi Portali del cittadino Richieste e prenotazioni SUAP Sportello Unico Attività Produttive Servizi INAIL Servizi INPS Tutte le categorie per Governo e settore pubblico)
Istruzione, cultura e sport (Finanziamenti Iscrizione a servizi Richieste e prenotazioni Servizi Audio, Video e Multimediali Servizi INAIL Servizi INPS Servizi Scuola e Università Servizi di pagamento, controllo pagamenti, tasse e tributi Visure, controllo e consultazione dati)
Popolazione e società (Anagrafe Finanziamenti Iscrizione a servizi Servizi Sociali e della Comunità Servizi di Certificazione e Autocertificazione Servizi di avvisi e notifiche Servizi di connettività pubblica Servizi per la viabilità)
Regioni e città (Portali del cittadino Visure, controllo e consultazione dati)
Salute (Anagrafe Fascicolo Sanitario Elettronico Servizi INAIL Servizi INPS Servizi Sanitari Visure, controllo e consultazione dati)

IDENTITY PROVIDER	LIVELLI DI SICUREZZA	AREA GEOGRAFICA	RICONOSCIMENTO DI PERSONA	RICONOSCIMENTO VIA WEBCAM	RICONOSCIMENTO CIE*, CNS	RICONOSCIMENTO FIRMA DIGITALE	Invio del codice OTP anche via sms	
aruba.it ID	1 2 3	IT EU	✓	A pagamento	✓	✓	Sì	⌄
InfoCert ID	1 2 3	IT EU	✓	A pagamento	✓	✓	Sì	⌄
intesa ID	1 2 3	IT EU	✓	A pagamento		✓	No	⌄
lepida	1 2 3	IT EU	✓	A pagamento - attivazione a breve	✓	✓	Sì	⌄
Namirial ID	1 2 3	IT EU	✓		✓	✓	Sì	⌄
Poste ID nuovo sistema spid	1 2 3	IT EU	In Ufficio Postale (gratis) A domicilio (a pagamento)		✓	✓	Sì	⌄
SIELTE id	1 2 3	IT EU	✓	✓	✓	✓	Sì	⌄
SpidItalia	1 2 3	IT EU		A pagamento	✓	✓	Sì	⌄
TIM id	1 2 3	IT EU	✓	A pagamento	✓	✓	Sì	⌄

* Sono accettate solo le Carte d'Identità Elettroniche 3.0, ovvero quelle che non hanno la banda ottica sul retro della tessera in plastica.

Bitcoin: la storia, come funziona ed il suo futuro

Cosa sono i Bitcoin?

Sono la prima valuta digitale decentralizzata.

La novità, anche se ormai questa valuta è in circolazione dal 2009, non è tanto nella digitalizzazione dei pagamenti, a cui tutti ormai, nell'era di Internet, siamo abituati, quanto al fatto che sia decentralizzata. Diversamente da tutte le monete tradizionali i bitcoin sfuggono a qualsiasi autorità: a coniarli non ci pensa la zecca dello Stato e non c'è alcuna Banca Centrale che ne controlli il valore né un intermediario finanziario che ne convalidi le transazioni.

Nato con l'intento di rendere più sicure e veloci le transazioni su internet, Bitcoin è un sistema per le transazioni elettroniche che non si basa più sulla fiducia in un'autorità terza, ma sulla matematica e sulla crittografia. La Banca centrale è sostituita dalla rete Bitcoin, un network di tipo peer-to-peer[1] (p2p) a cui tutti possono partecipare, a patto che si installi nel proprio computer il software omonimo, che è libero ed open-source[2], anche se è necessaria un'elevata potenza di calcolo. I nodi del network, facendo "girare" il software all'interno dei propri dispositivi, contribuiscono in modo diffuso a convalidare e registrare le transazioni tra due utenti che si vogliono scambiare delle unità di questo nuovo tipo di valuta, garantendone inoltre l'anonimato grazie alla crittografia insita nel sistema.

L'attività di validazione e registrazione delle transazioni è detta "mining", in italiano minare, un termine che ricalca metaforicamente l'attività di estrazione dell'oro da una miniera, e i nodi che la svolgono sono chiamati appunto "minatori". Tale attività sfrutta la potenza computazionale dei dispositivi dei minatori, ed è remunerata attraverso bitcoin[3] di nuova emissione, secondo un preciso sistema di ricompense.

Sono oltre 17 milioni e mezzo i bitcoin in circolazione al momento, mentre il valore di 1 BTC oggi[4] è di circa 3800$. Tale prezzo è determinato dal mercato, ovvero dal meccanismo della domanda e dell'offerta, ed è caratterizzato da una forte volatilità.

Usare bitcoin può sembrare facile come spedire e ricevere delle e-mail, capirne tutte le sfaccettature può risultare invece molto complicato, a seconda del grado di analisi cui si vuole pervenire. Le discipline interessate sono molteplici, tuttavia "Non c'è nulla a cui lo [Bitcoin] si possa paragonare", dice il suo stesso ideatore Satoshi Nakamoto[5].

"Bitcoin è la prima valuta digitale decentralizzata", dice il famoso video introduttivo di bitcoin.org, sito di riferimento della comunità Bitcoin, "Un'innovativa rete di pagamento e un nuovo tipo di denaro". Già da queste prime considerazioni si capisce come la parola Bitcoin racchiuda molteplici concetti.

Come detto Bitcoin (con la "B" maiuscola) è una rete di pagamento virtuale, ideata per velocizzare e rendere più sicure le transazioni su internet. All'interno di questo network viene scambiato un nuovo tipo di valuta, diverso dalle valute tradizionali a cui siamo abituati: i bitcoin (con la "b" minuscola). Diversità e innovazione risiedono nel fatto che questa "valuta" è decentralizzata, cioè manca un'unità organizzativa centrale che la controlli e ne gestisca l'emissione. La Banca Centrale Europea (BCE) è l'ente centrale che controlla l'euro attraverso l'attuazione della politica monetaria nei paesi dell'Euro Zona, similmente la Federal Reserve (Fed) controlla il dollaro statunitense, mentre in Bitcoin manca un soggetto adibito a tale controllo, sia questi un ente pubblico o privato. Come se non bastasse le transazioni di bitcoin non necessitano di appoggiarsi ad alcuna istituzione finanziaria che funga da terzo garante, presenza essenziale nel commercio online con scambi in valute tradizionali.

Tuttavia il controllo c'è, eccome.

Tale controllo è diffuso e distribuito nella rete, garantito dall'adesione ad un protocollo comune, un insieme di regole che definiscono il funzionamento del sistema, che si esplica nell'utilizzo del software Bitcoin. Ogni nodo del network, cioè ogni dispositivo hardware su cui lavora il software Bitcoin, e in grado di comunicare in rete con gli altri dispositivi, diventando un soggetto attivo nel processo di gestione della valuta. Tanto più numerosi sono i nodi tanto più il concetto di decentralizzazione è significativo. Si faccia attenzione che per utilizzare i bitcoin, per comprare prodotti o servizi online o semplicemente per inviare del

1 Peer-to-peer(p2p) o rete paritetica: architettura di rete informatica in cui I nodi sono tra loro paritetici, potendosi comportare sia da client che da server.

2 Open source: software di cui gli autori rendono pubblico il codice sorgente, permettendone lo sviluppo a chiunque.

3 Comunemente Bitcoin (con la B maiuscola) indica il sistema di pagamento, mentre bitcoin indica la valuta scambiata attraverso tale sistema.

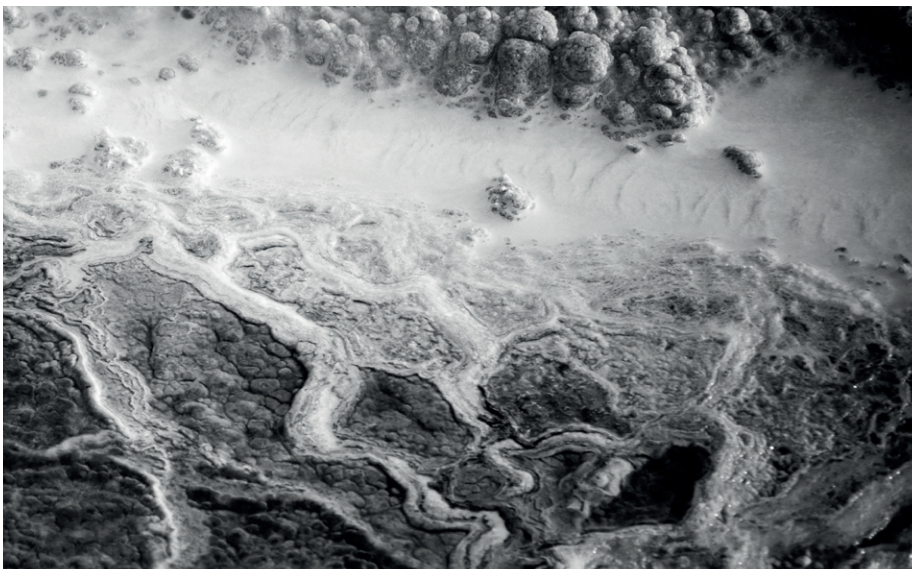
4 Prezzo in data 2 marzo 2019. Fonte: coinmarketcap.com

5 Si tratta di un post di Satoshi Nakomoto nell'ambito di una discussione su bitcointalk.org, forum di riferimento per la comunità Bitcoin. Il post è del 5 luglio 2010.

denaro ad un amico o parente, non è necessario essere un nodo di Bitcoin. I nodi sono necessari affinché le transazioni in bitcoin siano possibili, ma per i semplici utilizzatori della valuta non è obbligatorio partecipare attivamente alla rete, basta soltanto crearsi un indirizzo Bitcoin, simile ad un account per le e-mail.

Poiché il protocollo e il software sono stati comunque ideati e rilasciati dallo stesso inventore di Bitcoin, Satoshi Nakamoto, qualche scettico potrebbe benissimo sostenere che è il suo stesso ideatore l'autorità centrale, questione che si smentisce immediatamente considerando la natura libera e open-source del progetto. Bitcoin si pone infatti come aperto agli sviluppatori che vogliano apportare delle migliorie al progetto, tuttavia agli stessi sviluppatori risulta quasi impossibile forzare un profondo cambiamento del protocollo, in quanto ogni nodo è libero di scegliere quale software o versione utilizzare, al patto che siano conformi alle stesse regole e risultino compatibili con i software utilizzati dagli altri nodi. Quest'ultima caratteristica palesa la necessità di un consenso tra utilizzatori e sviluppatori affinché il sistema funzioni correttamente, e conseguentemente risulta assai arduo il tentativo di centralizzare il sistema, ovvero attribuire poteri regolamentari ad un'autorità centrale. Inoltre le qualità di risorsa libera ed aperta, se da un lato hanno aperto la strada allo sviluppo di nuove valute concorrenti sulla falsa riga di Bitcoin, dall'altro risultano essere fondamentali per la maturazione dell'intero sistema, grazie al considerevole valore intellettuale apportato da sviluppatori ed esperti di tutto il mondo.

In sintesi, si può dire che Bitcoin è un nuovo sistema di pagamento, in cui il controllo è distribuito e diffuso in maniera decentralizzata fra i nodi della rete, che facendo girare un apposito software regolato da uno specifico protocollo, rende possibili transazioni elettroniche in una nuova valuta digitale, i bitcoin. Bitcoin infine è un network, un protocollo ed anche una tecnologia che rende possibile il funzionamento di un sistema innovativo.



Bitcoin dal 2009 a oggi

Bitcoin nasce ufficialmente il 3 gennaio 2009 dalla mente di Satoshi Nakamoto, con l'uscita del primo client che da avvio all'attività di mining e conseguentemente alla creazione di nuove unità di valuta. Il 12 gennaio viene registrata nella blockchain la prima transazione in cui Satoshi invia 10 BTC ad Hal Finney, cypherpunk ed esperto di crittografia.

Bitcoin dal canto suo sembra proprio mettere in pratica le idee e gli obiettivi per cui è nato il movimento dei cypherpunks, ovvero per difendere il diritto alla privacy con la creazione di un sistema di pagamento anonimo alternativo a quelli tradizionali, attraverso la matematica e la crittografia.

Ma chi è realmente Satoshi Nakamoto? Non si sa, e probabilmente mai si potrà sapere l'identità dell'ideatore di Bitcoin, o forse del gruppo di persone che l'ha creato e che si nasconde dietro questo pseudonimo. Risalgono al 2011 le ultime notizie in merito a questo misterioso personaggio: una mail mandata agli sviluppatori e alla comunità Bitcoin in cui dice "Sono passato ad altro. È (Bitcoin) in buone mani con Gavin (Andresen, uno tra i primi sviluppatori ad unirsi a Bitcoin) e tutti gli altri", passando in qualche modo il testimone.

Nel 2010 nascono i primi Bitcoin Exchange, mentre a maggio dello stesso anno avviene il primo acquisto di un bene "reale": all'interno di bitcointalk.org, forum di riferimento della comunità Bitcoin, il programmatore Laszlo Hanyecz offre 10.000 BTC (pari all'epoca a 25$) in cambio di una pizza!!!

Nel febbraio 2011 il prezzo di 1 BTC arriva per la prima volta a quota 1$. Prezzo che a giugno passerà dai 10$ per 1 BTC al massimo di 31,91$ in soli quattro giorni, in quella che è chiamata "The Great Bubble of 2011", salvo poi scendere e stabilizzarsi attorno ai 5$ nei mesi successivi. Il 2011 è anche l'anno dell'apertura di Silk Road, piattaforma online di compravendita di droga e altri prodotti illegali in cambio di bitcoin per sfruttarne l'anonimità dei pagamenti, e dell'inizio dei primi attacchi hacker verso i siti di exchange, incentivati anche dall'aumento di prezzo della criptovaluta, che vedono sottrarre dai propri server decine di migliaia di bitcoin, senza la possibilità di rintracciare i responsabili. Episodi che certamente non contribuiscono alla diffusione di Bitcoin.

Negli anni 2012 e 2013 aumentano progressivamente i commercianti disposti ad accettare bitcoin, grazie anche alla diffusione di servizi volti a semplificarne le procedure di pagamento, e aumenta il numero di associazioni e progetti che li accettano in donazione. Ad inizio aprile 2013 il prezzo di 1 BTC supera quota 100$, arrivando circa dieci giorni dopo ad un massimo di 266$. A novembre il prezzo passa da 270$ a oltre 1000$ in pochi giorni, registrando il picco più alto dalla sua nascita a oggi.

Nel 2014 chiude per bancarotta MtGox, exchange leader fino ad allo-

ra del palcoscenico Bitcoin, oggetto di numerosi attacchi hacker che hanno complessivamente causato una perdita stimata attorno alle 850 mila unità di bitcoin, con gravi danni per i portafogli dei propri clienti.

Nonostante un brutto inizio il 2014 è stato sicuramente un anno positivo per quanto riguarda la diffusione e il progresso dell'economia di bitcoin, mentre il suo prezzo è andato progressivamente e stabilmente riducendosi. Importanti società come Microsoft, Dell hanno deciso di accettare i bitcoin come mezzo di pagamento, ma soprattutto Pay Pal decide di aprire al mondo della criptovaluta attraverso una partnership con BitPay, Coinbase e GoCoin, società che offrono servizi alle imprese per l'accettazione di bitcoin.

L'inizio del 2015 continua con la crescita degli investimenti, mentre il prezzo dopo un'iniziale discesa, negli ultimi mesi sembra dare maggiori segnali di stabilità oscillando tra i 250$ e i 750$ in tutto il 2016. E' nella primavera del 2017 che avvenne il rapido boom del prezzo di bitcoin fino al culmine della vera e propria bolla speculativa che oggi tutti noi conosciamo avendo portato il prezzo fino ad un massimo di 19.000$ nel dicembre 2017, con il conseguente scoppio del fenomeno delle Altcoins. Il 2018 rappresentò fin da subito lo scoppio di questa bolla speculativa, portando il prezzo di bitcoin e delle relative Altcoins ad un calo fino dell'80-90%. Nell'ultima parte del 2018 si è assistito ad una costanza nel prezzo di bitcoin tra i 6.000$ e i 7000$, fino ad un nuovo calo in Novembre toccando i minimi del periodo intorno ai 3.000$ ed una conseguente nuova fase di stabilità odierna tra i 4.000$ e i 5.000$.

Le Alternative Coins (Altcoins)

La caratteristica di open-source del progetto Bitcoin ha permesso la partecipazione di molti sviluppatori, che dal 2009 ad oggi hanno fornito un importantissimo contributo nello sviluppo del software e nella correzione delle vulnerabilità che via via si sono presentate.

La stessa caratteristica ha inoltre dato avvio alla nascita di numerose criptovalute alternative e in competizione con Bitcoin, dette anche altcoins. Secondo coinmarketcap.com ci sono attualmente più di 2000 criptovalute diverse in circolazione, tuttavia ne nascono di nuove ogni giorno mentre altre invece scompaiono. Bitcoin rimane la più importante e la più preziosa considerando una capitalizzazione di mercato intorno ai 80 miliardi di dollari in un mercato di 170 totali.

La maggior parte di queste criptovalute replicano molto similmente i meccanismi alla base di Bitcoin, mentre altre propongono diverse ed innovative funzionalità. Parliamo di realtà come Litecoin, Dash, Ripple, Stellar, Cardano etc.. Non entriamo in questo studio nei particolari e nelle specifiche di ogni singola altcoin senza entrare nelle specifiche tecniche del loro funzionamento.

Citiamo velocemente solo Ethereum definendola come una piattaforma decentralizzata diversa da Bitcoin in quanto consente la creazione e pubblicazione peer-to-peer di contratti intelligenti (smart contracts), che possono essere descritti come un insieme di codici informatici che automatizzano qualsiasi tipo di processo o transazione che gira sulla Blockchain.

Come funziona Bitcoin?

Il funzionamento di Bitcoin è nelle mani dei nodi del network detti "miners" (minatori). Questi, attraverso il processo di mining, collezionano le transazioni che avvengono in continuazione, ovviamente in bitcoin, all'interno di specifici recipienti chiamati blocchi. Questi blocchi sono uniti tra loro a formare la blockchain (o catena a blocchi), che rappresenta l'organo più importante e innovativo dell'intero sistema. La blockchain è un grande registro aperto agli utenti e condiviso, contenente ogni transazione avvenuta in bitcoin dalla sua nascita ad oggi al fine di risolvere il probelma del double-spending[6], e viene sottoposta a continuo aggiornamento da parte dei minatori. Chiunque può visualizzare una versione completa della blockchain, installando il software Bitcoin o più semplicemente sul web grazie ad appositi siti detti block explorer. Ciò nonostante Bitcoin garantisce alti livelli di anonimità, in quanto le transazioni avvengono tra indirizzi pseudonimi a partire dai quali è molto difficile risalire all'identità del suo utilizzatore.

Come affermato in precedenza, le transazioni di bitcoin avvengono tra indirizzi creati appositamente per questo scopo. Un bitcoin di fatto non esiste come unità a sé stante, come può esserlo una stringa di bit nel mondo digitale. Esistono solo transazioni tra indirizzi, con i rispettivi bilanci che aumentano o diminuiscono. Possedere dei bitcoin significa possedere la chiave privata associata ad almeno uno di questi indirizzi tale per cui, all'interno di un qualsiasi blocco "risolto" dal lavoro dei minatori, è stata in precedenza registrata una transazione a favore di quello specifico indirizzo. Ogni transazione di bitcoin è perfettamente tracciabile, in quanto ad ogni istante in cui si visualizzi la blockchain è possibile sapere quanti bitcoin appartengono ad un determinato indirizzo, ed inoltre è possibile risalire a quale indirizzo glieli abbia forniti, e da chi quest'ultimo li abbia a sua volta ricevuti. La blockchain rappresenta dunque la traccia, lo storico di tutte le transazioni. È uno strumento affidabile, che fa prova poiché nessuna transazione può risultare in conflitto con un'altra, poiché ogni transazione è irreversibile, cioè impossibile da annullare, e viene registrata e marcata temporalmente, per cui nessun utente può inviare bitcoin che non possiede o che ha già inviato a un altro indirizzo, risolvendo così il problema del double-spending.

Il Mining

Come rendere possibile un sistema di pagamento decentralizzato? Come sopperire alla mancanza di un'autorità centrale che stabilisca la politica mo-

6 Double-spending (doppia spesa): è la possibilità di spendere una stessa unità di valuta digitale più volte; nei sistemi di pagamento tradizionali questo problema è risolto dalla presenza degli intermediari finanziari che controllano le operazioni. In Bitcoin, mancando di un'autorità centrale, tale problema è risolto dalla presenza della blockchain e dal lavoro dei minatori, che conoscendo tutte le passate transazioni valide sono in grado di rigettare gli scambi che tentano di spendere dei bitcoin già spesi in passato.

netaria per quella determinata valuta? Come garantire e alimentare la fiducia in un sistema così diverso dai sistemi di pagamento tradizionali, soprattutto per la sensibilità del tema trattato, ovvero la sicurezza del nostro denaro? La risposta a tutte queste domande è il mining.

Spesso erroneamente si ricollega l'attività di mining alla sola produzione ed emissione di nuovi bitcoin, tuttavia non è questo il suo scopo principale. Il vero obiettivo di tale processo è mantenere l'integrità e l'autenticità della blockchain, che per gli utenti di Bitcoin rappresenta un vero e proprio conto bancario. Solo se questo registro mantiene le caratteristiche menzionate, chiunque possieda dei bitcoin può stare tranquillo che quel denaro gli appartiene; se invece si rivelasse fragile a tentativi di contraffazione, finalizzati per esempio a convalidare più transazioni tra loro inconsistenti (double- spending), la fiducia nel sistema svanirebbe e Bitcoin sarebbe destinato a fallire.

Ma da chi e come viene svolta questa attività? Teoricamente può essere svolta da tutti, a patto che si installi il client Bitcoin sul proprio computer. Il mining sfrutta la potenza di calcolo dei dispositivi hardware messi a disposizione dai nodi della rete, ed è stato ideato dallo stesso Nakatomo difficile e dispendioso in termini di tempi di elaborazione del calcolatore, in modo che vengano prodotti un certo numero di nuovi blocchi in un intervallo di tempo prefissato, a prescindere dal numero di transazioni che avvengono nel network. Infatti se nel network avvengono poche transazioni, queste non possono essere messe in attesa fino a che non si raggiunge una determinata soglia, altrimenti la praticità come sistema di pagamento svanirebbe; inoltre i primi blocchi minati non contenevano transazioni, eccetto le coinbase, allo scopo di creare e mettere in circolazione le prime unità di valuta.

Ad ogni produzione di un nuovo blocco viene emessa una quantità stabilita di nuovi bitcoin, che spettano al minatore che per primo l'ha prodotto. A tale quantità prestabilita va a sommarsi anche il totale delle commissioni delle transazioni registrate nel blocco.

In sintesi il mining è ideato per rendere sicura la blockchain, e tale sicurezza è resa possibile da quanti più nodi "onesti" sono presenti nel network, in modo da rendere difficile se non impossibile il lavoro dei nodi "disonesti" che vogliono invece modificare il registro a loro vantaggio per spendere più volte dei bitcoin già spesi. L'onestà dei nodi è "comprata" dallo stesso protocollo attraverso un particolare sistema di attribuzione di ricompense, che incentivano tale onestà.

Il motivo per cui questo processo si chiami mining vuole sottolineare la relazione tra i cercatori d'oro che impiegano sempre più sforzi per trovare nuove pepite d'oro, e i nodi che similmente impiegano sempre più potenza computazionale, costosa in termini di energia consumata, per aumentare i bitcoin in circolazione.

Le regole alla base del mining

La produzione di nuovi blocchi da agganciare alla blockchain e l'emissione di nuova moneta sono strettamente collegati, tali che ogni produzione di un nuovo blocco corrisponde ad una nuova emissione di un quantitativo prefissato di bitcoin. Tutto in Bitcoin è stabilito. Il tetto massimo di bitcoin in circolazione è anch'esso prestabilito, ed è (o meglio sarà) di circa 21 milioni di unità. Infine anche la quantità di nuovi bitcoin emessi ad ogni produzione di un nuovo blocco è fissata. Tale ricompensa si attestava originariamente in 50 BTC per blocco, e viene dimezzata progressivamente ogni 210.000 nuovi blocchi che equivalgono a circa 4 anni. Il primo dimezzamento si è verificato il 28 novembre 2012, per cui attualmente la ricompensa è quantificata in 12,5 BTC per blocco. Quando in futuro la ricompensa sarà prossima allo zero, l'unica remunerazione per i minatori saranno le commissioni di transazione.

Dove si "mettono" i bitcoin?

Ci sono diversi modi per ottenere dei bitcoin, alcuni semplici ed immediati, altri che richiedono un po' più di tempo ed organizzazione. Sono in continua crescita gli esercizi commerciali, sia fisici che online dove si possono spendere. Tuttavia prima di pensare a come ottenere e spendere dei bitcoin è necessario mettersi nelle condizioni di poterli ricevere, e una volta ricevuti di poterli tenere al sicuro, senza rischiare di perderli o di farseli "rubare". A questo scopo è necessario possedere un wallet Bitcoin, un portafoglio elettronico che, molto metaforicamente, svolge le stesse funzioni di un portafoglio materiale, cioè di custodia del nostro denaro che in questo caso è digitale.

I portafogli Bitcoin non sono proprio l'equivalente di un conto corrente, anche se l'interfaccia offerta dai diversi servizi di wallet consente di sapere in ogni momento il totale dei bitcoin posseduti e le movimentazioni in entrata ed uscita, come una sorta di estratto conto in tempo reale. I bitcoin non sono di fatto contenuti all'interno di un portafoglio, ma sono memorizzati in un registro aperto al pubblico, la blockchain, sotto degli specifici indirizzi appartenenti ai diversi utenti. Gli indirizzi sono punti di ricezione e invio, e si presentano sotto forma di codici alfanumerici (come ad esempio "1G1vTdCYjqb5gucmhNQH7yTBy9uPHC5Aht"), in modo da non contenere alcun riferimento dell'utente utilizzatore, facendo di Bitcoin un sistema di pagamento pseudonimo.

Le transazioni di bitcoin si basano sulla tecnologia della crittografia asimmetrica (o crittografia a chiave pubblica/privata). Attraverso il meccanismo crittografico delle firme digitali, solo il possesso della chiave privata autorizza l'utente a spendere i bitcoin associati all'indirizzo da essa derivato. Per questo motivo la chiave privata non deve essere resa pubblica, ma deve essere custodita per non correre il rischio di non poter più spendere i bitcoin relativi.

I portafogli Bitcoin custodiscono le chiavi private dell'utente, che gli permettono di spendere i bitcoin associati al preciso indirizzo che deriva dalla chiave pubblica che a sua volta deriva dalla chiave privata in oggetto; questo è ciò che avviene dietro le quinte. Infatti il wallet offre all'utente un'in-

terfaccia intuitiva, che gli permette di visualizzare il bilancio di bitcoin a sua disposizione di tutti gli indirizzi diversi che egli possiede, dandogli la possibilità di effettuare delle transazioni in uscita verso determinati beneficiari, o di ricevere dei pagamenti ad un determinato indirizzo.

Storia

Anche se i primi anni di vita di Bitcoin non sono stati molto entusiasmanti dal punto di vista della diffusione e dell'utilizzo di questo nuovo tipo di valuta, l'anno 2009 può essere considerato come una sorta di data spartiacque: da un lato rappresenta il raggiungimento di un importante traguardo tecnologico frutto dei numerosi progressi in ambito crittografico e informatico e di alcuni tentativi di valute alternative falliti o mai effettivamente implementati; dall'altro lato segna la nascita attorno a Bitcoin di un vero e proprio ecosistema, e il successivo proliferare delle Altcoins, ovvero valute digitali alternative nate dopo la nascita del progetto Bitcoin.

Fattori che determinano il prezzo del bitcoin

Come affermato in precedenza, il prezzo del bitcoin è determinato dal mercato, ovvero dal meccanismo della domanda e dell'offerta. Ma quali sono le dinamiche che muovono la domanda? O, detto in altri termini, quali sono i motivi per cui, in un determinato intervallo di tempo, un individuo desideri ottenere una certa somma di bitcoin piuttosto che tenersi i suoi dollari o euro?

Gli individui desiderano possedere dei bitcoin perché vi riconoscono un valore. Ogni individuo può riconoscervi diversi valori e di conseguenza avere diversi motivi per detenere delle unità di valuta. I principali valori individuabili sono:

- valori scientifico/tecnologici derivanti dall'innovazione apportata da Bitcoin, che configura un sistema senza precedenti; questa è stata la motivazione principale che ha condotto i primi utenti a entrare nel mondo dei bitcoin, quando ancora il suo prezzo era vicino allo zero;
- valori sociali derivanti dalle caratteristiche di decentralizzazione e pseudonimia del sistema Bitcoin, e quindi di indipendenza dalle banche e dai governi e di maggiore garanzia della privacy rispetto ai sistemi di pagamento tradizionali; inoltre i valori sociali derivanti dalla diffusione di Bitcoin tra gli individui: all'aumentare della diffusione cresce anche l'utilità del possedere dei bitcoin, poiché crescono le possibilità di un loro reale impiego;
- valori tecnico/funzionali derivanti dall'utilità e dall'efficacia di Bitcoin come sistema per i pagamenti, per la sua velocità, praticità e per tutti i vantaggi che possono derivare dall'utilizzo della criptovaluta, come ad esempio i bassi costi di transazione, o la possibilità di effettuare pagamenti in ogni parte del mondo comodamente da casa.

I principali fattori che conducono a variazioni della domanda di bitcoin, e quindi del suo prezzo sono:

- **L'interesse:**

la diffusione dell'informazione in merito a bitcoin e al mondo delle criptovalute condiziona positivamente il prezzo; confrontando le statistiche del numero di digitazioni della parola bitcoin su Google e Wikipedia con l'andamento del prezzo dei bitcoin si rileva che aumento dell'interesse e aumento del prezzo sarebbero correlati.

- **Le notizie:**

le notizie negative causano incertezza, e in un sistema non controllato da un'autorità centrale i loro effetti si fanno sentire maggiormente. Esempi di tali notizie sono stati i frequenti furti delle chiavi private dai server delle piattaforme di exchange; la diminuzione del prezzo in relazione a tali eventi è frutto della perdita di fiducia in generale. Al contrario le notizie positive possono creare effetti positivi nel prezzo nel lungo periodo, aumentando la diffusione della valuta e quindi della domanda.

- **L'utilizzo dei bitcoin per le transazioni reali:**

riguardano l'entità della diffusione di Bitcoin, determinata dal suo effettivo utilizzo per le transazioni. Poiché è proprio Bitcoin stesso a proporsi come sistema per i pagamenti alternativo, per analizzare il livello del suo utilizzo non ci si può limitare al volume delle transazioni giornaliere che vengono registrate nella blockchain, perché questo dato comprende sia gli scambi "reali", ovvero derivanti da operazioni di acquisto e vendita di beni o servizi, sia la movimentazione di bitcoin tra un indirizzo e l'altro appartenenti ad uno stesso utente.

- **L'utilizzo dei bitcoin per scopi speculativi:**

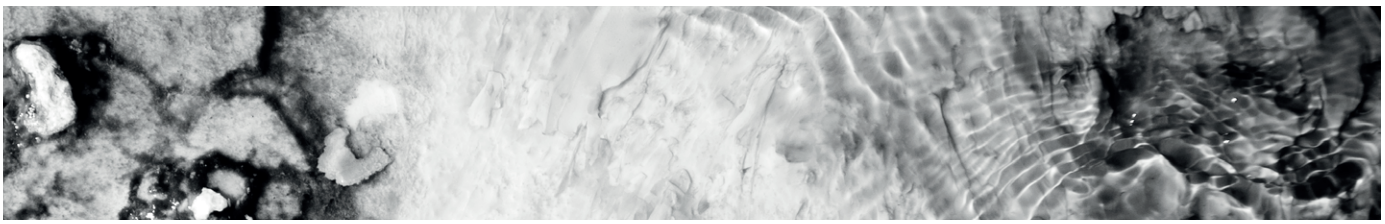
l'utilizzo di Bitcoin come investimento invece che come sistema per i pagamenti determina anch'esso effetti sul prezzo della criptovaluta; la presenza di investitori o speculatori può essere visto come benefico, perché si assumono il rischio di detenere delle unità di bitcoin al posto di altri utenti intimoriti dalla loro volatilità, ma il loro comportamento nel breve periodo sarebbe causa di maggiore instabilità.

Caratteristiche di bitcoin e principali differenze con le valute legali

Il report della BCE "Virtual Currency Scheme" di ottobre 2012 definisce come moneta legale (o moneta fiat) ogni valuta legale istituita e rilasciata da un'autorità centrale, accettata dalle persone in cambio di beni e servizi grazie alla fiducia che questi ripongono in quell'autorità, sottolineando come la fiducia sia l'elemento cruciale nei sistemi di moneta fiat.

La valuta bitcoin viene ricompresa all'interno della categoria delle valute virtuali, definite come monete digitali non regolate, istituite e controllate generalmente dai suoi sviluppatori ed accettate ed utilizzate tra i membri di specifiche comunità virtuali. Ci diversi tipi di monete virtuali a seconda della loro possibilità di interagire con il mondo reale, intesa come la possibilità di scambiarle con delle monete legali ad uno specifico tasso di cambio o di potervi acquistare beni e servizi nell'economia reale.

Per essere più precisi di quanto non abbia fatto la BCE nel suo report, bitcoin assieme ad altre valute simili



nate a partire dal 2009 sono da ricomprendersi all'interno della categoria delle criptovalute. Le criptovalute sono valute digitali indipendenti da qualsiasi unità centrale, che utilizzano la crittografia per verificare le transazioni e regolare l'emissione di nuove unità di valuta.

Le principali caratteristiche di bitcoin sono:

- **Decentralizzazione:**
  bitcoin non è stata istituita, né è controllata da alcuna autorità centrale. Il controllo sulle transazioni è eseguito da tante entità indipendenti in maniera decentralizzata e distribuita, per cui la presenza di banche e altri soggetti regolamentati non è più necessaria.

- **Non soggetta a politiche monetarie:**
  l'assenza di un'autorità centrale comporta anche l'impossibilità che un qualsiasi soggetto eserciti azioni coercitive sulla valuta, come ad esempio l'aumento o la diminuzione delle unità di valuta in circolazione. L'offerta di moneta è stabilita a priori dal protocollo, in maniera che aumenti progressivamente fino ad arrivare alla soglia massima di 21 milioni di unità.

- **Non ha corso legale:**
  i bitcoin sono accettati come mezzo di pagamento solo su base volontaria, e dunque non possono essere utilizzati per estinguere delle obbligazioni pecuniarie se il creditore si rifiuta di accettarli.

- **Pseudonima:**
  le transazioni avvengono tra indirizzi pubblici a partire dai quali è praticamente impossibile risalire alla reale identità della persona fisica o giuridica che processa lo scambio di bitcoin.

- **Trasparente:**
  tutte le transazioni sono registrate in un registro aperto al pubblico, la blockchain, che ognuno può visualizzare. Esplorando la blockchain è possibile sapere quanti di quanti bitcoin dispone un determinato indirizzo in un preciso istante temporale, potendo inoltre risalire agli indirizzi che glieli hanno forniti.

- **Bassi costi di transazione:**
  l'assenza di soggetti che intermediano nelle transazioni ha la conseguenza di abbatterne i costi. In media le transazioni prevedono un addebito al mittente di circa 0,20$[7] come commissione, ma l'importo

  può essere maggiore o nullo a seconda di certe condizioni specifiche, quali la richiesta di una transazione più rapida da parte del mittente.

- **Transazioni veloci e irreversibili:**
  ogni transazione di bitcoin impiega mediamente 10 minuti per essere confermata. Tali transazioni sono irreversibili, ovvero impossibili da annullare.

Il futuro di Bitcoin

Il bitcoin potrà sostituire le valute legali?

Secondo la tradizione economica la moneta deve essere in grado di soddisfare tre principali funzioni:

- **Riserva di valore:**
  la moneta deve essere in grado di conservare il proprio valore nel tempo affinché gli individui possano decidere se utilizzarla subito oppure accumularla per spenderla in futuro;

- **Mezzo di scambio:**
  la moneta deve svolgere la funzione di strumento di pagamento in cambio di beni e servizi, e deve essere comunemente accettata;

- **Unità di conto:**
  la moneta deve svolgere la funzione di unità di misura comune, attraverso la quale determinare il prezzo dei beni e facilitare la misurazione delle transazioni economiche.

Vediamo ora come si comporta il bitcoin rispetto alle funzioni appena delineate, e come potrebbe comportarsi in futuro.

Con riferimento alla prima funzione, ovvero quella di riserva di valore, non si è in grado in questo momento di stabilire se il bitcoin conserverà o meno il proprio valore in futuro. Nonostante sia previsto un limite nel totale delle unità di criptovaluta in circolazione, e tale limite assieme a tutte le altre regole stabilite dal protocollo risultino difficili da stravolgere attraverso delle sostanziali modifiche, non si può prevedere con certezza la futura domanda di bitcoin da parte degli individui, vera determinante del prezzo della criptovaluta.

La domanda futura di bitcoin dipenderà dal suo utilizzo futuro come strumento di pagamento. Il valore del bitcoin attualmente è troppo volatile da poter essere considerato uno strumento di riserva di valore, e risulta assai arduo prevedere se questa volatilità persisterà anche in futuro o se il bitcoin raggiungerà un livello di prezzo stabile.

La funzione di mezzo di scambio è quella che il bitcoin sembra attualmente poter soddisfare più di tutte le altre, quella per cui del resto è stata ideata dallo stesso Satoshi Nakamoto. Con Bitcoin si possono effettuare pagamenti in modo semplice, veloce, con elevati livelli di privacy e a costi bassi se confrontati con tutti gli altri sistemi di pagamento tradizionali.

Tuttavia la criptovaluta non è universalmente accettata come strumento di pagamento per beni e servizi, perciò è ancora difficile spenderli, ma sono in costante aumento gli esercizi commerciali, sia fisici che online, disposti ad accettarli, e di conseguenza sono in crescita gli individui desiderosi

7 Calcolando una "next block fee" con un'attesa standard di massimo 10min.

di utilizzarli. I volumi di denaro scambiati attraverso Bitcoin non sono che una modestissima frazione dei volumi totali scambiati tramite i sistemi per i pagamenti elettronici tradizionali, e tale frazione risulta ancora più infinitesimale se si considera che molte transazioni di bitcoin non riguardano l'acquisto di beni o servizi, ma sono processate solamente per fini speculativi.

Tuttavia, anche nell'ambito di questa seconda funzione non ci si può esimere da considerazioni riguardanti il futuro di Bitcoin. Considerando l'attività di mining e le modalità con cui viene remunerata, è necessario delineare gli scenari che potrebbero presentarsi in futuro quando le ricompense previste per la risoluzione di ogni blocco saranno quasi nulle, e l'unica fonte remunerativa sarà rappresentata dalle commissioni di transazione: la diffusione dei bitcoin come mezzo di pagamento potrebbe condurre ad un aumento del numero di transazioni giornaliere e quindi del totale dei ricavi derivanti dalle commissioni, compensando l'annullamento delle ricompense per i blocchi risolti; un altro possibile scenario potrebbe prevedere l'aumento del costo delle commissioni, annullando uno dei principali vantaggi derivanti dall'utilizzo della criptovaluta; il terzo scenario possibile prevedrebbe invece l'abbandono del mining da parte di numerosi individui o società poiché non più profittevole, con il rischio che tale attività e si concentri nelle mani di pochi soggetti o, nella peggiore delle ipotesi, che degeneri in un monopolio, cancellando la più innovativa caratteristica del sistema, ovvero la decentralizzazione. Dunque nemmeno il futuro utilizzo di bitcoin come mezzo di scambio è così certo, ed è difficile da prevedere in questo momento.

L'ultima funzione, ovvero quella di unità di conto, è difficilmente soddisfabile dal bitcoin nello stato attuale. L'elevata volatilità che caratterizza il prezzo della criptovaluta non ne consente un agevole utilizzo come unità di misura per determinare il valore dei beni. I commercianti dovrebbero aggiornare i prezzi dei beni in bitcoin anche più volte nell'arco della giornata, poiché il tasso di cambio con il dollaro o con altre valute legali cambia anche più volte nello stesso giorno. Per questo motivo i prezzi dei beni rimangono comunque nominati in valuta legale e convertiti in bitcoin al momento della vendita secondo il tasso di cambio corrente.

Da quanto emerso finora si può comprendere la difficoltà del bitcoin nel soddisfare in maniera esaustiva le tre funzioni che comunemente ci si aspetta da una moneta legale. Non essendoci un'autorità centrale che imponga l'utilizzo o l'accettazione del bitcoin come strumento di pagamento, il suo futuro non può che dipendere dalla volontà degli individui di utilizzarlo ed accettarlo.

Il primo dubbio è legato al persistere della forte volatilità del prezzo del bitcoin anche in futuro. Il tetto massimo prestabilito di unità di bitcoin in circolazione rende la sua curva di offerta inelastica, ovvero insensibile alle variazioni della domanda di criptovaluta degli individui, variazioni che vanno a riflettersi totalmente nel suo prezzo. Anche nell'ipotesi che il mercato scoprisse il reale valore del bitcoin come mezzo di scambio le variazioni della domanda di bitcoin determinerebbero delle fluttuazioni più o meno consistenti del prezzo, considerando che la domanda può variare in ragione di moltissimi fattori, dovuti per esempio alla stagionalità delle vendite o ai cicli economici. Se si rendesse l'offerta di bitcoin più elastica, per esempio aumentando o diminuendo le ricompense previste per la risoluzione dei blocchi in relazione al numero di transazioni processate in un determinato periodo di tempo antecedente, gli effetti delle variazioni della domanda si rifletterebbero lo stesso nel prezzo ma in maniera meno accentuata, garantendo maggiore stabilità, tuttavia questo richiederebbe una sostanziale modifica del protocollo e del disegno originale di Bitcoin.

Il bitcoin come mezzo di scambio potrebbe trovare ampia diffusione in futuro, tuttavia è ancora troppo presto per dirlo, considerando che il fenomeno delle criptovalute è ancora relativamente giovane. Fondamentale per tale diffusione sarà lo sviluppo dei servizi connessi al mondo della criptovaluta, che dovranno offrire maggiori garanzie di sicurezza e rendere, se possibile, ancora più facile ed accessibile tale mondo. Fondamentali saranno inoltre le decisioni dei Governi in merito alla qualifica normativa e fiscale entro cui ricomprendere Bitcoin e le altre criptovalute.

Tuttavia l'innovazione introdotta da Satoshi Nakamoto non si limita al mondo delle criptovalute e dei sistemi di pagamento, ma sembra destinata a sconvolgere molti altri sistemi tradizionalmente basati sulla fiducia in un'autorità centrale.

Ad oggi pare più conclamata e ad uno step successivo dell'implementazione di massa l'innovazione tecnologica che sta alla base di Bitcoin, ovvero la blockchain, un registro elettronico le cui informazioni sono protette crittograficamente e risultano impossibili da manomettere, e la cui autenticità è garantita non da un'autorità centrale bensì dagli utenti in maniera decentralizzata sulla base del consenso. Un organo potenzialmente in grado da solo di soppiantare le autorità centrali e gli intermediari di molti sistemi esistenti, la cui applicazione al sistema monetario rappresenta soltanto un primo e particolare tentativo di decentralizzazione possibile.

Se è possibile infatti trasferire del denaro in maniera decentralizzata, in maniera rapida e sicura, è anche possibile scambiare risorse digitali come per esempio azioni di una società, le obbligazioni ed altri strumenti di investimento.

Inoltre non solo gli intermediari finanziari, ma anche le società che offrono servizi di risorse digitali potranno essere rivoluzionate da questa nuova tecnologia disruptive. Bitcoin rappresenta infatti soltanto un punto di partenza, una killer-app per utilizzare un gergo informatico, ovvero una particolare applicazione di una determinata tecnologia il cui successo nel mercato ha l'effetto di aprire la strada ad altre diverse applicazioni della tecnologia stessa.

Lorenzo Negri

ceo di Cripton.it

Cari avvocati la realtà aumentata sta arrivando

(e vi riguarderà da vicino)

Qualche anno fa la stampa si divertiva (oggi possiamo dirlo... a sproposito) a favoleggiare di come la realtà aumentata avrebbe cambiato le nostre vite. Era l'epoca dei Google Glass, occhiali avveniristici in grado di fare due cose: mostrarci in tempo reale le notifiche e i messaggi che arrivavano al nostro smartphone e scattare foto o video semplicemente con un occhiolino. Luxottica si era aggiudicata contratti miliardari per portare questa tecnologia nei propri occhiali, sarebbero usciti nel 2013, no 2014, forse nel 2015... forse...

Dietro la parola forse c'è tutta la frustrazione di chi ha lavorato per anni a questi progetti. In realtà mai sopiti del tutto.

Da allora le applicazioni "civili" della realtà aumentata hanno lasciato l'ambito degli smartglass (occhiali intelligenti) e sono entrate nei nostri smartphone: facebook e snapchat sono le applicazioni più famose che usano questa tecnologia ma sono letteralmente centinaia le app che permettono di aumentare immagini reali con informazioni create digitalmente. Non mi soffermo su cosa è possibile fare: è sufficiente aprire il proprio smartphone per fare una foto aggiungendo orecchie da gatto o altri gadget ai video che registriamo. Divertente, rido spesso con mia figlia quando lo faccio... del resto è evidente che si tratta di un fake fatto apposta per sorridere in famiglia...

Oggi il fake è evidente ma sarà sempre così?

Il Washington Post ha denunciato che l'attrice Scarlett Johansson sta cercando in tutti i modi di bloccare i filmati a luci rosse che la ritraggono nel bel mezzo di un film hard... Film che l'attrice non ha mai girato. Unendo realtà aumentata e intelligenza artificiale è possibile realizzare video in cui digitale e reale si fondono senza che sia possibile distinguere dove finisce la realtà e dove inizia la fantasia.

Deep Fake è il nome della tecnologia e sappiamo che è solo questione di tempo prima che questa diventi disponibile al grande pubblico con conseguenze che oggi stentiamo a immaginare.

Torniamo a quello di cui stavamo parlando: quale è il reale stato dell'arte della realtà aumentata?

In ambito consumer al momento è relegata ai nostri smartphone con risultati interessanti anche se lontani da un realismo in grado di ingannare il pubblico.

In ambito industriale invece si stanno facendo passi avanti molto importanti: le due società più interessanti in questo ambito sono Magic Leap e Microsoft.

Magic Leap One è un visore per la realtà aumentata che assomiglia a un paio di occhiali ma permette di fondere la realtà con modelli tridimensionali posizionati nello spazio attorno a chi li indossa. Ho avuto la possibilità di utilizzarli qualche settimana fa e le cose che mi hanno maggiormente impressionato sono l'ampiezza della visuale e la possibilità di maneggiare un piccolo cacciavite con le mie mani... ogni volta che svitavo una vite avevo una piccola reazione che mi permetteva di immergermi ulteriormente nell'esperienza.

Microsoft Hololens è il visore di cui sentiremo parlare di più dall'anno prossimo quando uscirà la seconda versione. Non sono solito lasciarmi andare a facili ottimismi ma siamo vicini a un salto molto importante per questa tecnologia. Innanzitutto sarà possibile integrare questo visore con caschetti esistenti (quindi vedremo operai al lavoro con caschetti in realtà aumentata che forniranno loro informazioni per svolgere meglio il loro lavoro), inoltre sarà possibile "toccare" gli ologrammi creati attorno a noi rendendo possibile l'interazione con la realtà aumentata.

Se la persona accanto a me indossa un visore può accedere a diverse tecnologie che vanno anche ben oltre la semplice renderizzazione di gattini:

- Leggendo un testo con OCR (optical character recognition) il visore potrebbe rendere un documento "tradizionale" simile a un ipertesto utilizzato sui siti web: stai leggendo una sentenza per un tuo cliente? Il software mentre leggi il testo potrebbe scandagliare altre sentenze a suo carico e mostrartele permettendoti di navigare tra reale e digitale senza soluzione di continuità.

Un esempio è raccontato da questa società tedesca che sta utilizzando Hololens per supportare la lettura delle cifre dei contatori

https://anyline.com/news/first-holographic-ocr-scanner/.

Non solo ma è solo per scelta delle società produttrici se oggi questi occhiali non hanno la possibilità di riconoscere in tempo reale il viso della persona che stiamo incontrando. Sappiamo che queste tecnologie sono già in uso all'interno dei social network (da dove pensate che arrivino i suggerimenti su chi taggare in una foto facebook?).

- Il visore può immergerci in uno spazio tridimensionale partendo dall'osservazione di una immagine 2D. Immaginiamo ad esempio di leggere una perizia su un immobile e poterlo visitare come se ci trovassimo lì. Questo sarà ancora più semplice attraverso l'integrazione con BIM (building information modeling) obbligatorio negli appalti pubblici proprio da quest'anno.

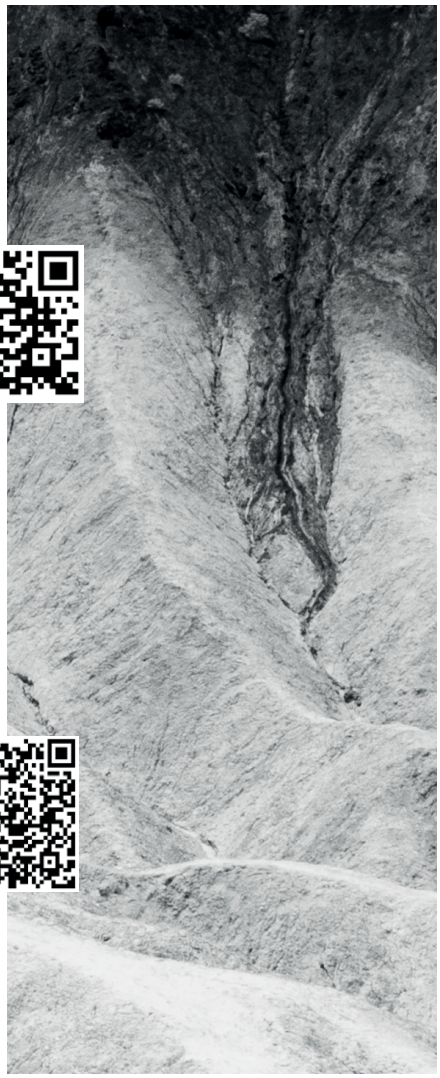
Esempi di questa tecnologia sono i cataloghi in realtà aumentata utilizzati in ambito crocieristico (MSC Crociere già dal 2016 sta sperimentando questo tipo di tecnologia) o industriale (nella nostra città anche Jbt ha una live brochure in AR).

http://www.bimholoview.com/

Tutti i lavoratori potranno beneficiare di queste tecnologie: non è un caso che l'esercito degli Stati Uniti abbia commissionato l'acquisto di 100.000 di questi visori nei prossimi 5 anni: non è un numero da capogiro ma questa commessa da sola vale il numero dei visori venduti da quando è stata lanciata. Come verranno utilizzati? Ancora non ci è dato di saperlo ma la protesta da parte dei dipendenti microsoft è arrivata fino alle orecchie del CEO Satya Nadella

https://thenewsrep.com/114727/microsoft-not-backing-out-of-us-army-contract-despite-protesting-workers/

Matteo Cavalieri
www.immersio.eu



CYBERCRIME & CYBERSECURITY

Gli impatti

Il 2017 è stato l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo, ma anche e soprattutto da quello qualitativo, evidenziando un trend di costante crescita degli attacchi, della loro gravità e dei danni conseguenti.

Il 2017 si è caratterizzato come "l'anno del trionfo del Malware, degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli. Ricordiamo le pesantissime interferenze di natura "cyber" avvenute durante le campagne presidenziali americana e francese, gli attacchi realizzati tramite centinaia di migliaia di device IoT (**I**nternet **o**f **T**hings). Il 2018 non è andato meglio del 2017 ed il 2019 "promette bene" per i cybercrime.

Purtroppo l'assordante silenzio di tutte le forze politiche sulle tematiche di sicurezza cibernetica non fa ben sperare, e anzi è sintomo di una drammatica mancanza di sensibilità in materia, che deve essere urgentemente ricondotta a dei livelli accettabili per un Paese tecnologicamente avanzato come il nostro, a fronte del rischio di un'ulteriore perdita di credibilità e competitività sul piano internazionale.

Buona lettura

Lucio Riva *

e Giovanni Tortorici **

* Legal Director Barilla

** Senior Manager Barilla

Sommario

Introduzione

La criminalità informatica (cybercrime) e la sicurezza informatica (cybersecurity) sono problemi che difficilmente possono essere separati in un ambiente interconnesso. La cybersecurity svolge un ruolo importante nello sviluppo continuo della tecnologia dell'informazione, nonché dei servizi basati su Internet. Migliorare la sicurezza informatica e proteggere le infrastrutture è essenziale per la sicurezza ed il benessere economico di ogni nazione. Rendere Internet più sicura e proteggere gli utenti di Internet dovrebbe diventare parte integrante dello sviluppo dei nuovi servizi ed essere argomento cardine della politica indirizzata verso innovazione e sviluppo.

Contrastare la criminalità informatica è una componente integrante di sicurezza informatica nazionale. È indispensabile l'adozione di una legislazione appropriata contro l'uso improprio delle ICTs (**I**nformation and **C**ommunications **T**echnology) per scopi criminali o di altro tipo e attività intese a pregiudicare l'integrità di infrastrutture critiche. A livello nazionale, questa è una responsabilità condivisa che richiede un coordinamento delle azioni relative alla prevenzione, alla preparazione, alla risposta ed al recupero da incidenti da parte delle autorità, del settore privato e dei cittadini.

Lo sviluppo di sistemi di protezione tecnica o l'educazione degli utenti a impedire che diventino vittime della criminalità informatica, può aiutare a ridurre il rischio dovuto alla criminalità informatica.

Lo sviluppo ed il supporto delle strategie di cybersecurity sono un elemento vitale nella lotta contro la criminalità informatica.

Le sfide legali, tecniche ed istituzionali poste dalla questione della sicurezza informatica sono globali e approfondite, e può essere affrontato solo attraverso una strategia coerente che tenga conto del ruolo delle diversi parti interessate, in un quadro di cooperazione internazionale.

Già nel 2007, l'ITU (**I**nternational **T**elecommunication **U**nion), organizzazione internazionale che si occupa di definire gli standard nelle telecomunicazioni e nell'uso delle onde radio, ha lanciato la GCA (**G**lobal **C**ibersecurity **A**genda) insieme a partner di governi, industria, organizzazioni locali ed internazionali, accademici e istituti di ricerca. Il GCA è un quadro globale per il dialogo e la cooperazione internazionale per coordinare la risposta internazionale alle crescenti sfide alla sicurezza informatica e migliorare fiducia e la sicurezza nella società dell'informazione. Si basa su lavoro, iniziative e partnership esistenti con l'obiettivo di proporre strategie globali per affrontare le sfide odierne legate alla costruzione di fiducia e sicurezza nell'uso delle ICTs. L'Agenda Global Cybersecurity ha obiettivi strategici principali, costruiti su cinque aree di lavoro:

1. Misure legali
2. Misure tecniche e procedurali
3. Strutture organizzative
4. Capacity Buidling
5. Cooperazione Internazionale

La lotta contro la criminalità informatica ha bisogno di un approccio globale. Dato che solo le misure tecniche non possono prevenire alcun crimine, è fondamentale che le forze dell'ordine possano indagare e perseguire efficacemente il crimine informatico. Tra le aree di lavoro GCA, le "Misure legali" si concentrano su come affrontare le sfide legislative poste dalle attività criminali commesse sulle reti ICTs in un modo compatibile a livello internazionale. Le "Misure tecniche e procedurali" si concentrano su misure chiave atte a promuovere l'adozione di approcci più efficaci per migliorare la sicurezza e la gestione dei rischi nel cyberspazio, compresi schemi di accreditamento, protocolli e standard. Le "Strutture organizzative" si focalizzano su prevenzione, individuazione, risposta e gestione delle crisi degli attacchi informatici, comprensa la protezione di sistemi critici di infrastruttura di informazione. "Capacity building" si concentra sull'elaborazione di strategie per meccanismi di "sviluppo delle capacità" per sensibilizzare, trasferire know-how ed aumentare la sicurezza informatica. Infine, la "cooperazione internazionale" si concentra sulla cooperazione internazionale, il dialogo e il coordinamento nel trattare con le minacce informatiche.

Tipologia e storia dei "cybercrime"

Il termine "cybercrime" viene utilizzato per coprire un'ampia varietà di condotta criminale. Comprende i reati riconosciuti una vasta gamma di reati diversi. È difficile sviluppare una tipologia o un sistema di classificazione per crimine informatico. Un approccio può essere trovato nella Convenzione Europea sulla criminalità informatica, che distingue tra quattro diversi tipi di reati:

1. reati contro la riservatezza, l'integrità e la disponibilità di dati e dei sistemi informatici;
2. reati informatici;
3. reati connessi al contenuto;
4. reati legati al copyright.

Questa tipologia non è del tutto coerente, in quanto non si basa su un unico criterio di differenziazione

tra categorie. Tre categorie si concentrano sull'oggetto della protezione legale: "reati contro la riservatezza, integrità e disponibilità di dati e sistemi informatici "; reati connessi al contenuto e reati legati al copyright. La quarta categoria di "reati informatici" non si concentra sull'oggetto di protezione legale, ma sul metodo utilizzato per commettere il crimine. Questa incoerenza porta a sovrapposizioni tra le categorie. Inoltre, alcuni termini utilizzati per descrivere atti criminali, come "cyber-terrorismo" o "Phishing", coprono atti che rientrano in diverse categorie. Tuttavia, le quattro categorie possono

servire come base di discussione per i cybercrime.

L'abuso criminale della tecnologia dell'informazione e la necessaria risposta legale sono problemi che sono stati discussi da quando è stata introdotta la tecnologia. Le prime soluzioni sono state implementane negli anni '50. Uno dei motivi per cui l'argomento rimane difficile è lo sviluppo tecnico costante, nonché i metodi ed i modi in cui i reati commessi sono in evoluzione.

Negli anni '60, l'introduzione di sistemi di computer basati su transistor, che erano più piccoli e meno costosi rispetto alle macchine basate su tubi a vuoto, ha portato ad un aumento nell'uso della tecnologia informatica. In questa fase iniziale, i reati erano focalizzati sul danno fisico ai sistemi informatici ed ai dati memorizzati. Per esempio, in Canada, nel 1969 una rivolta studentesca provocò un incendio e furono distrutti dati informatici distrutti ospitati presso il campus. A metà degli anni '60, gli Stati Uniti iniziarono un dibattito sulla creazione di un'autorità centrale di archiviazione dei dati per tutti i ministeri. In questo contesto, sono stati discussi gli abusi criminali delle banche dati ed i relativi rischi per la privacy.

Negli anni '70, l'uso dei sistemi informatici e dei dati informatici aumentò ulteriormente. Alla fine del decennio, un numero stimato di 100.000 computer mainframe operavano già negli Stati Uniti.

Con il calo dei prezzi, la tecnologia informatica è stata sempre più ampiamente utilizzata a tutti i livelli. Gli anni '70 furono caratterizzati da uno spostamento dai tradizionali crimini contro la proprietà che avevano dominato gli anni '60, a nuove forme di crimine sui sistemi informatici.

Mentre il danno fisico ha continuato ad essere una forma rilevante di abuso criminale contro i sistemi informatici, nuove forme di crimini per i computer sono state perpetrate e riconosciute. Includevano l'uso illegale dei sistemi informatici e la manipolazione di dati elettronici. Il passaggio dalle transazioni manuali a quelle informatizzate ha portato ad un'altra nuova forma di crimine: le frodi legate al computer. Già in quegli anni, enormi perdite finanziarie erano state causate da frode informatica. La frode informatica, in particolare, rappresentava una vera sfida per l'applicazione della legge e le autorità stavano investigando sempre più casi. L'applicazione della legislazione esistente in casi di criminalità informatica hanno portato a molte difficoltà. Un dibattito sulle soluzioni legali era iniziato in diverse parti del mondo. Gli Stati Uniti hanno discusso un progetto di legge studiato specificamente per affrontare la criminalità informatica.

L'Interpol ha discusso i fenomeni e le possibilità di risposta legale.

Negli anni '80, i personal computer sono diventati sempre più popolari. Con questo sviluppo, il numero di sistemi informatici e quindi il numero di potenziali obiettivi per i criminali è aumentato di nuovo. Per la prima volta, gli obiettivi includevano un'ampia gamma di infrastrutture critiche. Uno degli effetti collaterali della diffusione dei sistemi informatici è stato un crescente interesse per il software, con conseguente emergere delle prime forme di pirateria del software e crimini legati ai brevetti. L'interconnessione dei sistemi informatici ha portato nuovi tipi di crimini. Le reti hanno consentito ai trasgressori di entrare in un sistema informatico senza essere presenti sulla scena del crimine. Inoltre, con la possibilità di distribuire software attraverso le reti, i criminali abilitati a diffondere software dannoso come virus informatici verso nuove vittime. I paesi hanno iniziato il processo di aggiornamento della loro legislazione in modo da soddisfare i requisiti di un ambiente criminale in evoluzione. Anche le organizzazioni internazionali sono state coinvolte in questo processo.

L'OECD (**O**rganisation for **E**conomic **C**o-operation and **D**evelopment – da noi conosciuto anche come OCSE) ed il Consiglio Europeo hanno istituito gruppi di studio per analizzare i fenomeni e valutare possibilità di risposte legali.

L'introduzione dell'interfaccia grafica ("WWW") negli anni '90 è stata seguita da una rapida crescita del numero di utenti di Internet ed ha portato a nuove sfide. Informazioni legalmente rese disponibili in un paese erano quindi disponibili a livello globale, anche nei paesi in cui la pubblicazione di tali informazioni è stata criminalizzata. Un'altra preoccupazione associata ai servizi online che si è rivelata particolarmente difficile nell'indagine sul crimine transnazionale, è stata la velocità dello scambio di informazioni. Infine, la distribuzione di pornografia infantile è passata dallo scambio fisico di libri e nastri alla distribuzione online attraverso siti Web e servizi Internet.

Mentre i crimini informatici erano in generale reati locali, Internet si è rivelato un mezzo efficientissimo per lo sviluppo di crimini elettronici nel crimine transnazionale. Di conseguenza, la comunità internazionale ha affrontato la questione in modo più intenso. La Risoluzione dell'Assemblea Generale delle Nazioni Unite 45/121 adottata nel 1990 ed il manuale per la prevenzione ed il controllo dei reati informatici emesso nel 1994 sono solo due esempi. Come in ogni decennio precedente, le nuove tendenze nel campo della criminalità informatica hanno continuato a svilupparsi. Il primo decennio del nuovo millennio fu dominato da nuovi, altamente sofisticati metodi per commettere reati, come il "phishing", e gli "attacchi botnet". L'uso di tecnologie emergenti che sono più difficili da gestire ed investigare per le forze dell'ordine, come le comunicazioni VoIP (**V**oice-**o**ver-**IP**) ed il "cloud computing". Non sono solo i metodi che sono cambiati, ma anche gli impatti. Quando i criminali sono diventati in grado di automatizzare gli attacchi, il numero di reati è aumentato in modo significativo.

Qualche dettaglio tecnico tra attacco e difesa

Diciamo che non sempre il nemico è fuori dalla porta, ma a volte è in ”casa”. Pensiamo ai seguenti casi:

- Negligenza del dipendente
- Guasti ai sistemi di sicurezza
- Dispositivi mobili persi
- Ignoranza dei dipendenti su temi della sicurezza
- Smaltimento improprio di informazioni personali (per esempio nei cestini)
- Mancanza di educazione e consapevolezza
- Dipendenti in malafede

A tutto ciò dobbiamo comunque aggiungere realmente i nemici esterni:

- Gli hacker (malware, ransomware phishing / spear phishing)
- Ingegneria sociale
- Spionaggio aziendale
- I venditori di tecnologia
- Gli “Hacktivisti” politici,
- ecc....

Cerchiamo di elencare i cibercryme più diffusi:

Crimini “personali”

- Harrassment (molestie) che vanno dal cyberbullismo allo stalking
- Phishing, ossia messaggi email che sembrano autentici, ma sono falsi ed atti solo a carpire user e password
- Pharming, reindirizzamento di un sito web o dirottamento del dominio aziendale

Crimini Social Nertwork

- Adware e altri malware
- Email di notifica false
- Messaggi da amministratore sistema che richiedono la password
- Truffe dove si chiede “inviare denaro”, spesso in bitcoin
- Clickjacking – un clic sul link e questo malware pubblica link falsi sulla vostra webpage
- Script scam – inducono a fare un copia/incolla e lanciano script dannosi
- Frode, usando schemi che convincono a dare denaro
- Furto di identità – catturano quanto digitate per usarlo per inps, banche, carte di credito, ecc..

Crimini contro l’organizzazione

- Hacking, ossia trovare buchi nella sicurezza con vari intenti
- Hacktivism, hacking per fare dichiarazioni politiche
- Data breach, ossia violazione dei dati
- Cyber terrorism

Sarebbero necessari molte pagine per spiegare in dettaglio i vari cybercrime, ma senza scendere troppo in profondità, diamo un esempio di cosa si cela dietro la parola malware, indicandone le differenti tipologie. Essi Includono diversi tipi di programmi progettati per essere dannosi:

- Spam, invia email di massa non richieste
- Cookies, si Installano senza autorizzazione ed aiutano i siti Web a identificare il vostro ritorno, tenendo traccia dei siti web e delle pagine che visitate per indirizzare meglio gli annunci. Può raccogliere informazioni che non volete condividere
- Adware, crea Popup o banner pubblicitari per generare reddito; usa i cicli della CPU e la larghezza di banda di Internet, riducendo le prestazioni del PC
- Spyware, che raccoglie in segreto informazioni personali e solitamente viene installato per caso. Può anche dirottatore il browser
- Virus, un programma che si replica ed infetta i computer. Ha bisogno di un file host. Può utilizzare un programma di posta elettronica per infettare altri computer, ma sfrutta anche altre vie. L'attacco è chiamato payload.
- Logic Bomb, si comporta come un virus, ma non si replica. Esegue azioni dannose. Attacca quando sono soddisfatte determinate condizioni
- Time Bomb, è una "bomba logica" con innesco ad un determinato tempo
- Worms, è auto-replicante, ma non ho bisogno di un host per viaggiare. Viaggia su reti per infettare altre macchine.
- Botnet, rete di computer "zombi" o "bot" controllati da un master. Notifiche di sicurezza false
- Attacchi di tipo Denial of Service. Blocca un server o una rete inviando traffico eccessivo
- Trojan horses (cavalli di Troia). Sembra essere un programma legittimo. In realtà è dannoso
- Potrebbe installare adware, una barra degli strumenti, un keylogger o aprire una backdoor
- Ransomware. malware che impedisce di utilizzare il computer fino a quando non si paga una multa o una commissione, di solito in Bitcoin, una valuta anonima, digitale e crittografata.
- Rootkit. Set di programmi che permette a qualcuno di ottenere il controllo sul sistema. Nasconde il fatto che il computer sia stato compromesso Quasi impossibile da rilevare. Ha il comportamento di mascherarsi come altri malware.

Sembrerebbe che non ci sia scampo, ma in realtà esistono diversi modi per difendersi. Esistono i firewall, dispositivo hardware/software che bloccano l'accesso alla rete per determinate porte applicative e su specifici computer. I programmi antivirus proteggono da virus, trojans, worms, spyware.

I programmi antispyware proteggono ed analizzano il sistema evitando l'instalalzione di adware e spyware. Oggi esistono Security Suite che includono tutte queste funzioni.

Le stesse reti di comunicazione possono utilizzare crittografia e proteggersi al meglio, ma è una situazione che si evolve in continuazione, dove i criminali cercano di compiere le proprie azioni approfittando delle vulnerabilità dei sistemi e della mancanza di preparazione degli utenti.

La sfida della lotta al cybercrime

Molte comunicazioni quotidiane dipendono dalle ICT e dai servizi basati su Internet, comprese le chiamate VoIP o le e-mail. Le ICT sono ora responsabili delle funzioni di controllo e gestione in edifici, automobili e servizi aerei. La fornitura di energia, acqua e servizi di comunicazione dipende dalle ICT. L'ulteriore integrazione delle ICT nella vita di tutti i giorni continuerà probabilmente e la crescente fiducia sulle ICT rende i sistemi ed i servizi più vulnerabili agli attacchi informatici. Le strategie devono essere formulate per prevenire tali attacchi e sviluppare contromisure, tra cui lo sviluppo e la promozione di mezzi tecnici di protezione, nonché leggi adeguate e sufficienti per consentire alle forze dell'ordine di combattere efficacemente la criminalità informatica.

Sono necessarie solo attrezzature di base per commettere reati informatici. Commettere un reato richiede hardware, software ed accesso a Internet.

Per quanto riguarda l'hardware, la potenza dei computer è in continua crescita. Ci sono un certo numero di iniziative per consentire alle persone nei paesi in via di sviluppo di utilizzare le ICT in modo più ampio. I criminali possono impegnarsi in gravi crimini informatici con solo tecnologie informatiche economiche o di seconda mano: la conoscenza conta molto più che l'attrezzatura. La data della tecnologia informatica disponibile ha poca influenza sull'uso di quella attrezzatura per commettere crimini informatici. Commettere crimini informatici può essere facilitato attraverso strumenti software specialistici. I trasgressori possono scaricare strumenti software progettati per individuare porte di comunicazione aperte o proteggere la password.

L'ultimo elemento vitale è l'accesso a Internet. Sebbene il costo dell'accesso a Internet sia più alto nella maggior parte dei casi pae-

si in via di sviluppo che nei paesi industrializzati, il numero di utenti Internet nei paesi in via di sviluppo stanno crescendo rapidamente. I trasgressori generalmente non sottoscriveranno un servizio Internet per limitarne la durata e la possibilità di essere identificati, ma preferiscono servizi che possono utilizzare senza registrazione (verificata).

Un modo tipico di accedere alle reti è il cosiddetto "wardriving". Il termine descrive l'atto di andare in giro ricerca di reti wireless accessibili. I metodi più comuni che i criminali possono utilizzare per accedere alla rete in modo abbastanza anonimo è costituita da terminali Internet pubblici, reti aperte (wireless), reti hackerate e servizi prepagati senza requisiti di registrazione. Le forze dell'ordine stanno prendendo provvedimenti per limitare l'accesso incontrollato ai servizi Internet in modo da evitare un abuso criminale di questi servizi. In Italia e in Cina, ad esempio, l'uso di terminali Internet pubblici richiede l'identificazione degli utenti. Tuttavia, ci sono argomenti contro tali requisiti di identificazione. Sebbene la restrizione dell'accesso possa prevenire i reati e facilitare le indagini delle forze dell'ordine, tale legislazione potrebbe ostacolare la crescita della società dell'informazione e dello sviluppo dell'e-commerce. È stato suggerito che questa limitazione all'accesso a Internet potrebbe violare i diritti umani.

Ad esempio, la Corte europea ha emesso in una serie di casi sulla trasmissione che il diritto alla libertà di espressione si applica non solo al contenuto delle informazioni, ma anche ai mezzi di trasmissione o ricezione. Poiché ogni restrizione imposta ai mezzi interferisce necessariamente con il diritto di ricevere e impartire informazione, se questi principi vengono applicati a potenziali limitazioni sull'accesso a Internet, è possibile che tali approcci legislativi potrebbero comportare la violazione dei diritti umani.

Le indagini ed il perseguimento della criminalità informatica presentano una serie di sfide per l'applicazione della legge. È vitale non solo educare le persone coinvolte nella lotta contro la criminalità informatica, ma anche a produrre una bozza di una legislazione nazionale adeguata ed efficace.

Una legislazione adeguata è la base per l'indagine e il perseguimento della criminalità informatica. Tuttavia, i legislatori devono rispondere continuamente agli sviluppi di Internet e monitorare l'efficacia delle esistenti disposizioni, in particolare data la velocità degli sviluppi nella tecnologia di rete.

Storicamente, l'introduzione di servizi informatici o di tecnologie legate a Internet ha dato origine a nuove forme di crimine, subito dopo l'introduzione della tecnologia. Un esempio è lo sviluppo di reti di computer negli anni '70: il primo accesso non autorizzato alle reti di computer è avvenuto in brevissimo tempo. Allo stesso modo, i primi reati di software sono comparsi poco dopo l'introduzione del personal computer negli anni '80, quando questi sistemi venivano usati per copiare i prodotti software.

Ci vuole tempo per aggiornare la legge penale nazionale per perseguire nuove forme di criminalità informatica online. Anzi, alcuni i paesi non hanno ancora finito con questo processo di adeguamento. Reati che sono stati criminalizzati sotto la legislazione penale nazionale devono essere rivisti e aggiornati. Ad esempio, le informazioni digitali devono avere status equivalente a quello delle firme e delle stampe tradizionali. Senza l'integrazione dei reati della criminalità informatica, le violazioni non possono essere perseguite. La principale sfida per gli ordinamenti penali nazionali è il ritardo tra il riconoscimento del potenziale abuso di nuove tecnologie e le modifiche necessarie alla legge penale nazionale. Questa sfida rimane pertinente ed attuale quanto la velocità di innovazione della rete accelera. Molti paesi stanno lavorando duramente per raggiungere gli adeguamenti legislativi. In generale, il processo di aggiustamento ha tre passi: adeguamento alla legislazione nazionale, identificazione delle lacune nel codice penale e redazione di una nuova legislazione.

Strategie anti cybercrime: la cybersicurezza

Il crescente numero di cybercrime riconosciuti e gli strumenti tecnici per automatizzare i reati informatici (inclusi i sistemi anonimi di condivisione file) ed i prodotti software progettati per lo sviluppo di virus per computer, indicano

che la lotta contro la criminalità informatica è diventata un elemento essenziale per l'applicazione della legge a livello mondiale. La criminalità informatica è una sfida per le forze dell'ordine sia in paesi sviluppati, sia in paesi in via di sviluppo. Poiché le ICTs si evolvono così rapidamente, specialmente nei paesi in via di sviluppo, la creazione e l'attuazione di un'efficace strategia anti-cybercrime come parte di una strategia di sicurezza informatica è essenziale e la legislazione sulla cybercriminalità è parte integrante di una strategia di sicurezza informatica

Come accennato in precedenza, la cybersecurity svolge un ruolo importante nello sviluppo continuo di tecnologia dell'informazione, nonché dei servizi Internet. Rendere Internet più sicuro e proteggere gli utenti Internet è diventato parte integrante dello sviluppo di nuovi servizi e lo stesso percorso lo deve seguire anche la politica governativa. Ad esempio, lo sviluppo di sistemi di protezione tecnica o l'educazione degli utenti per impedire che diventino vittime della criminalità informatica, può aiutare a ridurre il rischio di cybercrime.

Una strategia anti-cybercrime dovrebbe essere un elemento integrante di sicurezza informatica. L'Agenda per la sicurezza informatica dell'ITU, come quadro globale per il dialogo e la cooperazione internazionale lavora per coordinare la risposta internazionale alle crescenti sfide alla sicurezza informatica e per aumentare la fiducia e la sicurezza nella società dell'informazione. Si basa sul lavoro, le iniziative e le partnership esistenti, con l'obiettivo di proporre strategie globali per affrontare queste sfide correlate. Tutte le misure richieste, evidenziate nei cinque pilastri del Global Cybersecurity Agenda sono rilevanti per qualsiasi strategia di cybersecurity. Inoltre, la capacità di lottare efficacemente contro la criminalità informatica richiede l'adozione di misure in tutte e cinque le aree indicate nel paragrafo introduttivo.

Una possibilità è che possano essere introdotte le strategie anti-cybercrime già sviluppate nei paesi industrializzati, nei paesi in via di sviluppo, offrendo vantaggi di costi e tempi ridotti per lo sviluppo stesso della strategia. L'attuazione delle strategie esistenti potrebbe consentire ai paesi in via di sviluppo di beneficiare delle conoscenze esistenti e dell'esperienza. Ciononostante, l'attuazione di una strategia anti-cybercrime esistente pone una serie di difficoltà. Anche se sfide analoghe si affrontano sia in paesi in via di sviluppo che in quelli sviluppati, le soluzioni ottimali che potrebbe essere adottate dipendono dalle risorse e dalle capacità di ciascun paese. I paesi industrializzati possono essere in grado di promuovere la sicurezza informatica in modi diversi e più flessibili, ad esempio concentrandosi su problemi di protezione tecnica con costi più elevati.

Ci sono molte altre questioni che devono essere prese in considerazione dai paesi in via di sviluppo che adottano strategie anti-cybercrime esistenti, Alcune questioni includono la compatibilità dei rispettivi sistemi legali, la possibilità di sostenere le iniziative (ad esempio l'educazione della società), la portata delle misure di autoprotezione in essere, nonché l'entità del sostegno del settore privato (ad esempio attraverso partenariati pubblico-privato).

Data la natura internazionale della criminalità informatica, l'armonizzazione delle leggi e delle tecniche nazionali è essenziale nella la lotta contro il crimine informatico. Tuttavia, l'armonizzazione deve tener conto della domanda locale e delle capacità. L'importanza degli aspetti locali nell'attuazione delle strategie anti-cybercrime è sottolineato dal fatto che molti standard legali e tecnici sono stati concordati tra paesi industrializzati e non comprendono vari aspetti importanti per i paesi in via di sviluppo. Pertanto, i fattori locali e le differenze devono essere incluse nella implementazione della strategia.

Lo sviluppo di una legislazione per criminalizzare determinati comportamenti o introdurre strumenti di indagine è piuttosto importante, ma si tratta di un processo insolito per la maggior parte dei paesi. La procedura regolare è innanzitutto quella di introdurre una policy. Una policy è comparabile ad una strategia che definisce i diversi strumenti utilizzati per affrontare la questione. A differenza di una strategia generale di cybercrime che può rivolgersi a vari stakehol-

der, il ruolo della policy è definire la risposta pubblica del governo ad un determinato problema. Questa risposta non è necessariamente limitata alla legislazione: i governi hanno vari strumenti che possono essere utilizzati per raggiungere gli obiettivi della policy.

Si potrebbe anche includere una legislazione più incentrata sulla prevenzione della criminalità. A questo proposito, lo sviluppo di una policy consente al governo di definire in modo completo la risposta del governo stesso ad un problema. La lotta contro la criminalità informatica non può mai limitarsi ad introdurre una legislazione, ma contiene varie strategie con diverse misure, la policy può garantire che quelle diverse misure non causino conflitti. Nell'ambito di diversi approcci per armonizzare la legislazione in materia di criminalità informatica, non è stata data una priorità troppo bassa solo integrando la legislazione nel quadro giuridico nazionale, ma includendola anche in una policy esistente, o nello sviluppo di tale policy per la prima volta.

Di conseguenza alcuni paesi che si sono limitati ad introdurre legislazione sulla criminalità informatica senza aver sviluppato una strategia anti-cybercrime e policy in materia, hanno affrontato gravi difficoltà. Erano principalmente il risultato di una mancanza di prevenzione della criminalità con una sovrapposizione tra diverse misure.

Policy, cooperazione ed informazione

L'introduzione della legislazione sulla criminalità informatica non è un compito facile in quanto vi sono varie aree che richiedono una regolamentazione. Nel diritto penale sostanziale e nel diritto procedurale, la legislazione in materia di criminalità informatica può comprendere questioni correlate alla cooperazione internazionale, alle prove elettroniche ed alla responsabilità di un fornitore di servizi Internet (ISP). Nella maggior parte dei paesi possono già esistere elementi di tale legislazione, spesso in diversi quadri giuridici.

Le disposizioni relative alla criminalità informatica non devono necessariamente essere implementate in un'unica parte di legislazione. Per quanto riguarda le strutture esistenti, potrebbe essere necessario aggiornare diverse parti di legislazione o rimuovere le disposizioni di una legge precedente nel processo di introduzione della nuova legislazione.

Questo approccio di attuazione della legislazione sulla criminalità informatica attraverso un processo di rispetto delle strutture esistenti è sicuramente più impegnativo del semplice implementare uno standard locale o una "best practice" internazionale, parola per parola in un atto legislativo autonomo. Ma riguardo al fatto che questo processo di personalizzazione consente di mantenere le tradizioni giuridiche nazionali, molti paesi favoriscono tale approccio.

La policy può essere utilizzata per definire i diversi componenti che devono essere integrati ed identificati in leggi esistenti che richiedono aggiornamenti.

Nonostante il fatto che le minacce di sanzione possano potenzialmente prevenire i crimini, il fulcro della legislazione penale lo è non sulla prevenzione della criminalità, ma sul crimine sanzionatorio. Tuttavia, la prevenzione della criminalità è identificata come un componente chiave in una lotta efficace contro la criminalità informatica. Le misure possono variare da soluzioni tecniche fino al blocco dell'accesso a contenuti illegali.

Esistono due diversi modelli per stabilire le azioni nella lotta alla criminalità informatica, vale a dire: interpretare estensivamente le leggi esistenti o creare nuove leggi. Due aree tradizionali di coinvolgimento dei piani regolatori, sono la protezione dei consumatori e la sicurezza della rete.

Con il passare dai servizi di telecomunicazione ai servizi connessi a Internet, l'attenzione della protezione del consumatore è cambiata. Oltre alle tradizionali minacce, è necessario prendere in considerazione l'impatto di spam, software dannoso e botnet. In un ambiente convergente in cui le telecomunicazioni tradizionali e le autorità di regolamentazione possono lottare per risolvere alcuni problemi, come il consolidamento tra contenuti multimediali e fornitori di servizi di telecomunicazione, un piano regolatore convergente sembra essere in una posizione migliore per affrontare i problemi dei contenuti della rete. Inoltre, il piano regolatore convergente può aiutare ad evitare incoerenze ed incertezza della regolamentazione e l'intervento normativo iniquo rispetto al diverso contenuto consegnato su varie piattaforme. Tuttavia, nella discussione dei vantaggi di una convergenza, l'autorità di regolamentazione non dovrebbe compromettere l'importanza delle attività dei regolatori del settore informatico.

Quando si pensa di estendere l'interpretazione dei mandati esistenti, si deve prendere in considerazione la capacità del piano regolatore e la necessità di evitare sovrapposizioni con i mandati di altre organizzazioni. Come i potenziali conflitti che possono essere risolti più facilmente se i nuovi mandati sono chiaramente definiti. Il secondo approccio è la creazione di nuovi mandati. In considerazione dei potenziali conflitti, alcuni paesi hanno deciso di ridefinire i mandati per evitare confusione e sovrapposizioni.

L'organo competente ad adottare la legislazione è il legislatore, non un'autorità di regolamentazione.

Come primo passo ci sono le necessarie disposizioni sostanziali di diritto penale per criminalizzare atti come frode informatica, l'accesso illegale, l'interferenza dati, le violazioni del copyright e la pedopornografia. Il fatto che tali disposizioni esistono nel codice penale

che si applicano ad atti analoghi commessi al di fuori della rete non significa che possano essere applicati anche ad atti commessi su Internet. Pertanto, un'analisi approfondita delle attuali leggi nazionali è fondamentale per identificare eventuali lacune.

Oltre alle disposizioni sostanziali di diritto penale, per l'applicazione della legge sono necessari gli strumenti e servono anche i mezzi per indagare sulla criminalità informatica. Tali indagini stesse presentano una vera sfida. Gli autori dei reati possono agire da quasi tutti i luoghi del mondo ed adottare misure per mascherare la propria identità. Gli strumenti necessari per investigare il crimine informatico possono essere molto diversi da quelli utilizzati per indagare sui reati ordinari. A causa della dimensione internazionale del crimine informatico, è in aggiunta necessario sviluppare il quadro giuridico nazionale per poter cooperare con le forze dell'ordine anche all'estero.

Quando si tratta di criminalità informatica, le autorità investigative competenti, nonché i tribunali, devono occuparsi di prove elettroniche. Affrontare tali prove presenta una serie di novità, ma si aprono anche nuove possibilità di investigazione per il lavoro di esperti forensi e tribunali. In quei casi dove non sono disponibili altre fonti di prova, la capacità di identificare e perseguire con successo un trasgressore può dipendere dalla corretta raccolta e valutazione delle prove elettroniche. Ciò influenza il modo in cui esperti e tribunali si occupano di tali prove. Mentre i documenti tradizionali vengono introdotti consegnando il documento originale in tribunale, in alcuni casi è richiesta la prova digitale con procedure specifiche che non consentono la conversione in prove tradizionali. Avere una legislazione in vigore che si occupa dell'ammissibilità delle prove digitali è quindi considerato vitale nella lotta contro la criminalità informatica.

A causa della dimensione transnazionale di Internet e della globalizzazione dei servizi, il numero crescente di crimini informatici ha una dimensione internazionale. Paesi che desiderano cooperare con altri paesi che indagano sulla criminalità transnazionale dovranno utilizzare gli strumenti della cooperazione internazionale. Tenendo conto della mobilità dei trasgressori, l'indipendenza dalla presenza del reo e dell'impatto del reato, mostra la sfida e la necessità di una collaborazione di forze dell'ordine e autorità giudiziarie. A causa delle differenze nella legislazione nazionale e strumenti limitati, la cooperazione internazionale è considerata una delle principali sfide di una globalizzazione della criminalità. Un approccio globale per affrontare il crimine informatico deve essere perseguito nei paesi che devono prendere in considerazione il rafforzamento della loro capacità di cooperare con altri paesi e rendere la procedura più efficiente.

Il crimine informatico può difficilmente essere commesso senza l'uso dei servizi di un Internet Service Provider (ISP). Le e-mail con contenuti minacciosi vengono inviate utilizzando il servizio di un provider di posta elettronica e i contenuti illegali scaricati da un sito Web comportano tra l'altro il servizio di un fornitore di servizi di hosting e di un provider di accesso. Di conseguenza, gli ISP sono spesso al centro di indagini criminali che coinvolgono criminali che usano i servizi degli ISP per commettere un reato. Tenendo conto che, da un lato, la criminalità informatica non può essere operare senza il coinvolgimento degli ISP, ma d'altra parte, i fornitori spesso non ne hanno la capacità di fermare i criminali.

Prevenire questi crimini, ha portato alla domanda se la responsabilità dei provider di Internet ha bisogno di essere limitata. Questo problema può essere affrontato nell'ambito di un approccio legale completo alla criminalità informatica.

Le indagini relative al crimine informatico spesso hanno una forte componente tecnica. Inoltre, l'l'obbligo di mantenere l'integrità delle prove durante un'indagine richiede procedure precise. Lo sviluppo delle capacità necessarie e delle procedure è quindi un requisito necessario nella lotta contro la criminalità informatica. Un altro problema è lo sviluppo di sistemi di protezione tecnica. I sistemi informatici ben protetti sono più difficili da attaccare. Migliorare la protezione tecnica implementando adeguati standard di sicurezza è un primo passo importante. Le misure tecniche di protezione dovrebbero comprendere tutti gli elementi dell'infrastruttura tecnica: l'infrastruttura di rete principale, così come i molti computer connessi individualmente in tutto il mondo. È possibile identificare due potenziali gruppi target dar proteggere tra gli utenti di Internet e le aziende: gli utenti finali e le imprese da un lato (approccio diretto) ed i fornitori di servizi e le società di software. Dal punto di vista logistico, può essere più facile concentrarsi sulla protezione dell'infrastruttura principale, piuttosto che l'integrazione di milioni di utenti in una strategia anti-cybercrime.

La protezione può essere ottenuta indirettamente, assicurando i servizi che i consumatori utilizzano, come l'online banking. Questo approccio indiretto alla protezione degli utenti di Internet può ridurre il numero di persone e istituzioni che devono essere inclusi nei passaggi per promuovere la protezione tecnica. Anche se potrebbe sembrare limitante il numero di persone che devono essere incluse nella protezione tecnica auspicabile, gli utenti di computer ed Internet sono spesso l'anello più debole e l'obiettivo principale dei criminali. È spesso più facile attaccare i computer privati per ottenere informazioni sensibili piuttosto che sistemi informatici ben protette di in istituto finanziario.

Nonostante i problemi logistici, la protezione dell'utente finale è vitale per la protezione tecnica dell'intera rete.

I fornitori di servizi Internet ed i venditori di prodotti (ad esempio società di software) svolgono un ruolo fondamentale nel supporto delle strategie anti-cybercrime. A causa del loro contatto diretto con i clienti, possono operare come garanti di attività di sicurezza (ad esempio la distribuzione di strumenti di protezione ed informazioni sullo stato corrente di più recenti truffe).

Una lotta efficace contro la criminalità informatica richiede strutture organizzative altamente sviluppate. Senza avere le strutture giuste, quelle che evitano la sovrapposizione e si basano su chiare competenze, renderanno possibile effettuare indagini complesse che richiedono l'assistenza di diversi aspetti legali ed esperti tecnici.

La criminalità informatica è un fenomeno globale. Per essere in grado di investigare efficacemente i reati, le leggi devono essere armonizzate e serve sviluppare strumenti di cooperazione internazionale. Al fine di garantire standard globali sia nei paesi sviluppati che in quelli in via di sviluppo, è necessario creare capacità. Oltre alla creazione di capacità, è necessaria la formazione degli utenti.

Alcuni crimini informatici, specialmente quelli in relazione alle frodi, come "phishing" e "spoofing"[1],[2] generalmente non dipendono dalla mancanza di informazioni tecniche di protezione, ma piuttosto su una mancanza di consapevolezza da parte delle vittime.

Esistono vari prodotti software che possono identificare automaticamente siti Web fraudolenti, ma fino ad ora questi prodotti non possono identificare tutti i siti Web sospetti. Una strategia di protezione dell'utente basata solo su prodotti software è limitata alla capacità di proteggere gli utenti. Sebbene le misure di protezione tecnica continuino a svilupparsi ed a essere disponibili i prodotti vengono aggiornati regolarmente, ma tali prodotti non possono ancora sostituire altri approcci.

Uno degli elementi più importanti nella prevenzione della criminalità informatica è l'educazione dell'utente.

Ad esempio, se gli utenti sono consapevoli che i loro istituti finanziari non li contatteranno mai tramite e-mail richiedendo password o password i dettagli del conto bancario, non possono essere vittime di attacchi di phishing o di frodi di identità. L'educazione digli utenti di Internet riducono il numero di potenziali obiettivi. Gli utenti possono essere educati attraverso campagne pubbliche, lezioni in scuole, biblioteche, centri informatici ed università, nonché partenariati pubblico-privati. Un requisito importante di un'efficace strategia di educazione e informazione è la comunicazione aperta delle ultime minacce alla criminalità informatica. Alcuni stati e/o imprese private si rifiutano di sottolineare che i cittadini ed i clienti sono rispettivamente colpiti da minacce di criminalità informatica, al fine di evitare che perdano la fiducia nei servizi di comunicazione online. Per determinare il livello della minaccia, serve informare gli utenti, ed è fonda-

1 Art. 615 ter C.P. - Accesso abusivo ad un sistema informatico o telematico.-Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Si rinvia alla Direttiva n. 2016 /1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante le "misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" meglio nota come "Direttiva NIS (acronimo di Network and Information Security) La direttiva stabilisce misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno. In sostanza la direttiva ha posto l'obbligo a tutti gli stati membri di strategia nazionale in materia di sicurezza della rete e dei sistemi informativi, imponendo anche l'obbligo di istituzione di un gruppo di cooperazione strategica tra gli stati membri, nonché la nomina di un Autorità nazionale per ciascun stato membro quale punto di contatto.
La suddetta direttiva è stata recepita nel nostro ordinamento con D. Lgs 18 maggio 2018 n. 65.
La normativa italiana disciplina in particolare il settore energetico, dei trasporti, delle banche e dei mercati finanziari, nonché le infrastrutture digitali, i motori di ricerca e le piattaforme e-commerce.
Detto decreto istituisce l'Autorità Nazionale competente per settore, in materia di sicurezza delle reti e dei sistemi informativi (NIS) che in sostanza sono i ministeri preposti ai predetti settori economici (es. il Ministero dello Sviluppo Economico per il settore energia).
Viene altresì istituito presso la Presidenza del Consiglio dei Ministri, il CSIRT (Gruppi di intervento per la sicurezza informatica in caso d'incidente) che ha tra i propri compiti la definizione delle procedure per la prevenzione e la gestione degli incidenti informatici.
In determinati casi il CSIRT, d'intesa con l'autorità nazionale NIS, è tenuto a procedere alle informazioni dovute anche alle altre autorità dei diversi paesi e può informare il pubblico in relazione ai singoli incidenti.
A tal riguardo si richiama Il Regolamento di Esecuzione 151/2018 del 20 gennaio 2018 della Commissione che disciplina ulteriormente gli elementi che fornitori di servizi digitali devono porre in essere per garantire un livello di sicurezza adeguato delle reti e dei sistemi informativi e, tra questi, anche i parametri da adottare al fine di valutare la rilevanza di un incidente informatico e l'eventuale necessità di attivare la procedura di notifica.
Il predetto obbligo di informazione si correla con le disposizioni di cui agli artt. 33, 34 del Regolamento Europeo 679/2016 (GDPR) che stabiliscono rispettivamente: i) in caso di violazione dei dati personali, a carico del titolare del trattamento dei dati, il dovere di informare l'autorità nazionale di protezione dei dati (Garante Privacy); ii) nel caso in cui il data breach possa mettere a rischio i diritti e le libertà delle persone fisiche (es furto di identità, danno d'immagine, frode), l'obbligo di informare anche tutti gli interessati.

mentale migliorare la raccolta e la pubblicazione delle informazioni pertinenti.

In molti casi, i processi di trasferimento dei dati in Internet riguardano più di un paese. Questo è il risultato del design della rete ed il fatto che i protocolli garantiscano il successo delle trasmissioni, anche se le linee dirette sono temporaneamente bloccate (Internet nacque per scopi militari). Inoltre, un gran numero di servizi Internet (come ad esempio servizi di hosting) sono offerti da società che hanno sede all'estero. Nei casi in cui l'autore del reato non ha sede nello stesso paese della vittima, l'inchiesta richiede la cooperazione tra le forze dell'ordine in tutti i paesi interessati. Indagini transnazionali senza il consenso delle autorità competenti nei paesi interessati sono difficili per quanto riguarda il principio della sovranità nazionale. Questo principio non consente in generale ad un paese di svolgere indagini all'interno del territorio di un altro paese senza il permesso delle autorità locali. Pertanto, le indagini devono essere svolte con il sostegno delle autorità di tutti i paesi coinvolti. Per quanto riguarda il fatto che nella maggior parte dei casi c'è solo un intervallo di tempo molto breve disponibile in cui possono svolgersi indagini con successo, con applicazione del classico mutuo legale, ci sono chiare difficoltà quando si tratta di indagini sulla criminalità informatica. Questo è dovuto al fatto che, l'assistenza giudiziaria in generale richiede lunghe procedure formali. Di conseguenza, il miglioramento in termini di cooperazione internazionale rafforzata svolge un ruolo importante e critico nello sviluppo e nell'implementazione di strategie di cybersicurezza e strategie anti-cybercrime.

Risposte legali

In questo paragrafo forniremo una panoramica della risposta legale al fenomeno della criminalità informatica al fine di spiegare gli approcci giuridici nella criminalizzazione di determinati atti.

Le definizioni sono un elemento comune dei vari quadri giuridici. Comunque sono importanti per distinguere tra le diverse funzioni che hanno quelle definizioni. È in generale possibile dividere le definizioni in due classi: definizioni descrittive e statutarie. Descrittive sono le definizioni usate per spiegare il significato di parole ambigue, mentre le definizioni statutarie intendono sottoporre quelli che sono soggetti alla legge ad una particolare definizione di una parola.

La seguente panoramica non distingue tra questi due tipi di definizione. I quadri giuridici locali e le leggi modello non seguono solo concetti diversi per quanto riguarda il tipo di definizioni, ma anche quando si tratta di aspetti quantitativi.

Diamo di seguito alcune definizioni, in una lista assolutamente non esaustiva.

Fornitore di accesso (ISP): qualsiasi persona fisica o giuridica che fornisce un servizio elettronico;

Caching Provider: provider di memorizzazione nella cache - forniscono un servizio importante per aumentare la velocità di accesso ai contenuti;

Dati del computer: significa qualsiasi rappresentazione di fatti, informazioni o concetti in una forma adatta all' elaborazione in un sistema informatico, incluso un programma adatto a far sì che un sistema informatico esegua una funzione;

Dispositivo di archiviazione dei dati del computer: indica qualsiasi articolo o materiale (ad esempio un disco) dal quale le informazioni possono essere riprodotte, con o senza l'ausilio di altri articoli o dispositivi;

Computer System: indica un dispositivo o un gruppo di dispositivi interconnessi o correlati, incluso Internet, uno o più dei quali, in base ad un programma, esegue l'elaborazione automatica dei dati o di qualsiasi altra funzione;

Infrastruttura critica: significa sistemi informatici, dispositivi, reti, programmi per computer, dati del computer, così vitali per il paese che l'incapacità o la distruzione o l'interferenza con tali sistemi avrebbero per le attività un impatto debilitante sulla sicurezza nazionale o economica, sulla salute pubblica, o qualsiasi combinazione di questi argomenti.

Crittografia: significa scienza della protezione delle informazioni, in particolare per lo scopo di garantire la riservatezza, l'autenticazione, l'integrità e il non disconoscimento;

Dispositivi: includono, ma non in modo esaustivo i componenti di sistemi informatici quali a) schede grafiche, memoria, chip; b) componenti di archiviazione come dischi rigidi, schede di memoria, compact disc, nastri; c) dispositivi di input quali tastiere, mouse, trackpad, scanner, fotocamere digitali; d) dispositivi di output come stampante, schermi

Hindering (ostacolare):

a) tagliare la fornitura di energia elettrica ad un sistema informatico;

b) causare interferenze elettromagnetiche ad un sistema informatico;

c) corrompere un sistema informatico con qualsiasi mezzo;

d) immettere, trasmettere, danneggiare, cancellare, deteriorare, alterare o sopprimere dai del computer.

Hosting provider: indica qualsiasi persona fisica o giuridica che fornisce un servizio di trasmissione elettronica di dati memorizzando le informazioni fornite da un utente del servizio.

Hyperlink: significa caratteristica o proprietà di un elemento come simbolo, parola, frase, o immagine che contiene informazioni su un'altra fonte e punta ad essa per visualizzare un altro documen-

to quando viene eseguito.

Intercettazione: include ma non è limitato all'acquisizione, visualizzazione ed acquisizione di dati dal computer tramite cavo, wireless, sistema elettronico, ottico, magnetico, orale o altro, durante trasmissione attraverso l'uso di qualsiasi dispositivo tecnico.

Interferenza: termine standard utilizzato in diverse disposizioni relative alla criminalità informatica. Tuttavia, in diversi strumenti locali il termine è usato solo nei titoli di alcune disposizioni, ma non descrive un atto criminalizzato stesso.

Messaggi di posta elettronica multipli: significa un messaggio di posta che include e-mail e messaggi istantanei inviati a più di mille destinatari.

Software forense remoto: indica un software investigativo installato su un sistema informatico ed utilizzato per eseguire attività che includono, ma non sono limitate, alla registrazione dei tasti o alla trasmissione di un indirizzo IP.

Seize: che comprende (a) creare e conservare una copia dei dati del computer, anche utilizzando apparecchiature in loco; (b) rendere inaccessibili, o rimuovere, i dati del computer nel sistema informatico a cui si accede; (c) eseguire una stampa dell'output dei dati del computer.

Service Provider: qualsiasi ente pubblico o privato che fornisce agli utenti del proprio servizio la capacità di comunicare mezzi di un sistema informatico, e qualsiasi altra entità che elabora o memorizza dati informatici per conto di tale servizio di comunicazione o utenti di tale servizio.

Traffico dati: che si riferisce ad una comunicazione per mezzo di un sistema informatico; (b) è generato da un sistema informatico che fa parte della catena di comunicazione; (c) mostra l'origine della comunicazione, la destinazione, l'itinerario, la data, la dimensione, la durata o il tipo di comunicazione servizi sottostanti.

Lo sviluppo delle reti di computer, in virtù della loro capacità di collegare i computer ed offrire agli utenti accesso ad altri sistemi informatici, ha favorito gli hacker per scopi criminali.

C'è una sostanziale variazione nelle motivazioni degli hacker. Gli hacker non devono essere presenti sulla scena del crimine: hanno solo bisogno di eludere la protezione che protegge la rete. In molti casi di accessi illegali, i sistemi di sicurezza che proteggono la posizione fisica dell'hardware di rete sono più sofisticati rispetto ai sistemi di sicurezza che proteggono le informazioni sensibili sulle reti, anche nello stesso edificio. L'accesso illegale ai sistemi informatici ostacola gli operatori informatici nella gestione, nella normale operatività e nel controllo dei loro sistemi. Lo scopo della protezione è di mantenere l'integrità dei sistemi informatici. È fondamentale distinguere tra accesso illegale e reati successivi[3] (come lo spionaggio di dati), poiché le disposizioni legali hanno un diverso obiettivo di protezione.

Nella maggior parte dei casi, l'accesso illegale (dove la legge cerca di proteggere l'integrità del sistema informatico stesso) non è l'obiettivo finale, ma piuttosto un primo passo verso ulteriori crimini, come la modifica o l'acquisizione di dati memorizzati (dove la legge cerca di proteggere l'integrità e la riservatezza dei dati). La domanda è se l'atto di accesso illegale che debba essere criminalizzato, oltre a quello successivo. L'analisi dei vari approcci alla criminalizzazione dell'accesso illegale al computer a livello nazionale mostra che le disposizioni emanate talvolta confondono l'accesso illegale con i reati successivi. Alcuni paesi criminalizzano il semplice accesso,

3 **Art. 615 quarter C.P. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici** o telematici Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.
La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.
Art. 615 quinquies C.P. - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico. Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

mentre altri limitano la criminalizzazione solo ai reati in cui il sistema di accesso è protetto da misure di sicurezza o laddove l'autore del reato abbia intenzioni dannose[4] o in cui siano stati ottenuti i dati, o siano stati modificati o danneggiati. Altri paesi non criminalizzano l'accesso stesso, ma solo successivamente le eventuali conseguenze dello stesso. Gli oppositori alla criminalizzazione dell'accesso illegale si riferiscono a situazioni in cui non c'erano pericoli creati da una semplice intrusione, o dove atti di "hacking" hanno portato alla scoperta di scappatoie e debolezze (bugs) nella sicurezza dei sistemi informatici presi di mira.

La Convenzione del Consiglio d'Europa sulla criminalità informatica comprende una disposizione sull'accesso illegale che protegge l'integrità dei sistemi informatici criminalizzando l'accesso non autorizzato ad un sistema. La Convenzione sulla criminalità informatica offre la possibilità di limitazioni che, almeno nella maggior parte dei casi, consente ai paesi senza legislazione di mantenere leggi più liberali in materia di accessi illegali. La disposizione mira a proteggere l'integrità dei sistemi informatici.

Ciascuna Parte adotterà le misure legislative e di altro tipo che saranno necessarie per stabilire come reato i reati previsti dalla propria legislazione nazionale, se commessi intenzionalmente, l'accesso all'intero o a parte di un sistema informatico senza averne diritto. Una Parte può richiedere che il reato venga commesso violando le misure di sicurezza, con l'intento di ottenere dati informatici o altri intenti disonesti, o in relazione a un sistema informatico connesso ad un altro sistema informatico.

Il termine "accesso" non specifica un determinato mezzo di comunicazione, ma è aperto a ulteriori sviluppi tecnici. Comprenderà tutti i mezzi per accedere ad un altro sistema informatico, compresi gli attacchi Internet, e l'accesso illegale alle reti wireless. Anche l'accesso non autorizzato ai computer che non sono connessi a nessuna rete (ad es. aggirando la protezione tramite password) sono coperti dalla disposizione.

Questo approccio ampio implica che l'accesso illegale non riguarda solo i futuri sviluppi tecnici, ma copre anche i dati segreti a cui si accede da parte di addetti ai lavori e dipendenti.

La seconda frase dell'articolo 2 offre la possibilità di limitare la criminalizzazione dell'accesso illegale all'accesso al network. Gli atti illeciti ed i sistemi protetti sono così definiti in un modo che rimane aperto agli sviluppi futuri. Il Rapporto esplicativo elenca hardware, componenti, dati memorizzati, directory, traffico e dati relativi al contenuto come esempi delle parti di sistemi informatici a cui è possibile accedere.

Come tutti gli altri reati definiti dalla Convenzione del Consiglio d'Europa sulla criminalità informatica, l'articolo 2 richiede che l'autore del reato stia commettendo intenzionalmente i reati. La Convenzione sulla criminalità informatica non contiene una definizione del termine "intenzionalmente". Nella relazione esplicativa, i redattori hanno sottolineato che "Intenzionalmente" dovrebbe essere definito a livello nazionale.

L'accesso ad un computer può essere perseguito solo in base all'articolo 2 della Convenzione sulla criminalità informatica, se è avvenuto "senza diritto". L'accesso ad un sistema che consente l'accesso libero ed aperto al pubblico o l'accesso a un sistema con l'autorizzazione del proprietario o altri detentori dei diritti non è considerato "senza diritto". Oltre all'oggetto del libero accesso, viene anche affrontata la legittimità delle procedure di test di sicurezza. Gli amministratori del network e le società di sicurezza che testano la protezione dei sistemi informatici per identificare potenziali lacune nelle misure di sicurezza erano diffidenti nei confronti del rischio di criminalizzazione in caso di accesso illegale. Nonostante il fatto che questi professionisti generalmente lavorano con il permesso del proprietario e quindi agiscono legalmente, i redattori della Convenzione sulla criminalità informatica hanno sottolineato che "i test o la protezione della sicurezza di un sistema informatico autorizzato dal proprietario o dall'operatore, sono "con diritto". Il fatto che la vittima del reato abbia consegnato una password o un codice di accesso simile all'autore del reato non significa necessariamente che l'autore del reato abbia agito correttamente quando ha avuto accesso al sistema di computer della vittima. Se l'autore del reato ha persuaso la vittima a rivelare una password o un codice di accesso tramite un

4 **Art. 635 bis C.P. Danneggiamento di informazioni, dati e programmi informatici** - Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.
Art. 635 ter C.P. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità - Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.
Art. 635 Quater C.P. - Danneggiamento di sistemi informatici o telematici - Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.
Art. 635 quinquies C.P. - Danneggiamento di sistemi informatici o telematici di pubblica utilità - Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

approccio di social-engineering di successo, è necessario verificare se l'autorizzazione data dalla vittima copre l'atto compiuto dall'autore del reato. In generale, questo non è il caso e quindi l'autore del reato agisce "senza diritto".

In alternativa all'approccio generale, la Convenzione sulla criminalità informatica offre la possibilità di limitare la criminalizzazione con elementi aggiuntivi, elencati nella seconda frase. La procedura su come utilizzare questa riserva è prevista dall'articolo 42 della Convenzione sulla criminalità informatica. Possibili riserve riguardano le misure di sicurezza, intento speciale per ottenere dati informatici, altri intenti disonesti che giustificano la colpevolezza criminale, o requisiti che il reato possa essere commesso contro un sistema informatico attraverso un network. Un approccio simile può essere trovato nella decisione quadro del Consiglio dell'UE1450 relativa agli attacchi contro sistemi di informazione.

La Convenzione del Consiglio d'Europa sulla criminalità informatica, fornisce soluzioni legali solo per l'intercettazione illegale.

E' discutibile se l'articolo 3 della Convenzione del Consiglio d'Europa sulla criminalità informatica si applichi ad altri casi rispetto a quelli in cui vengono commessi reati intercettando i processi di trasferimento dei dati. L'articolo 3 della Convenzione sulla criminalità informatica non riguarda le forme di spionaggio di dati diverse dall'intercettazione dei processi di trasferimento.

Una questione spesso discussa in questo contesto è la questione se la criminalizzazione di accessi illegali rende superflua la criminalizzazione dello spionaggio dei dati.

Nei casi in cui l'autore del reato ha accesso legittimo ad un sistema informatico (ad es. perché gli viene ordinato di ripararlo) e in questa occasione (in violazione della legittimazione limitata) copia i file dal sistema, in genere l'atto non è coperto dalle disposizioni che criminalizzano l'accesso illegale. Dato che molti dati vitali sono ora memorizzati nei sistemi informatici, è essenziale valutare se i meccanismi esistenti per proteggere i dati sono adeguati o se sono necessarie altre disposizioni di legge penale per proteggere l'utente dallo spionaggio dei dati.

Oggi, gli utenti di computer possono utilizzare vari dispositivi hardware e strumenti software per proteggere le informazioni segrete. Possono installare firewall e sistemi di controllo degli accessi o crittografare le informazioni memorizzate e quindi ridurre il rischio di spionaggio dei dati. Sebbene sia di facile utilizzo sono disponibili dispositivi che richiedono solo una conoscenza limitata da parte degli utenti, con una protezione dei dati veramente efficace. Su un sistema informatico si richiede invece la conoscenza che solo pochi utenti hanno. I dati memorizzati su un computer privato, in particolare, spesso non sono adeguatamente protetti dallo spionaggio dei dati.

Conclusioni

I cybercrime sono estremamente diffusi perché la diffusione stessa dei computer e delle applicazioni ha creato una grande platea di potenziali vittime.

La grande mancanza di conoscenza è seconda solo alla convinzione di essere preparati che molti utenti purtroppo hanno.

Installare un'applicazione (app) è un'attività talmente semplice da non richiedere alcuna conoscenza specifica, ma rende le vittime consce di essere grandi esperte di informatica: così proliferano gli attacchi.

I sistemi si stanno evolvendo per diventare sempre più "protetti" ed automatizzati, ma di pari passo crescono anche gli attacchi sia in numero che in qualità.

Gli attacchi arrivano da tutti i paesi del mondo e non è facile avere una legge che sia dinamica come lo sono gli attacchi. Se come avviene sovente, gli attacchi sono transnazionali, perseguire i criminali informatici diventa cosa non semplice.

La base di tutto è creare consapevolezza e cultura, supportate poi da policy e leggi snelle e veloci: sembra una banalità, ma tutto ciò è di una complessità estrema e richiederà molto tempo.

Impariamo pian piano almeno a proteggerci con un po' di sano buon senso.

Giovanni Tortorici **

* Legal Director Barilla

** Senior Manager Barilla

seconda copertina

CRONACHE DAL FORO PARMENSE

g.c. di APE Parma Museo della FONDAZIONE MONTEPARMA

Attività del Consiglio

Dal 22 novembre 2018 al 20 febbraio 2019 il Consiglio si è riunito dieci volte.
Elenco delle presenze dei Consiglieri alle adunanze:

avv. Ugo Salvini	n. 10
avv. Elisa Gandini	n. 10
avv. Enrico Maggiorelli	n. 10
avv. Simona Brianti	n. 9
avv. Giuseppe Bruno	n. 10
avv. Vittorio Cagna	n. 10
avv. Francesco Giuseppe Coruzzi	n. 9
avv. Paola De Angelis	n. 9
avv. Matteo de Sensi	n. 9
avv. Daniela Francalanci	n. 10
avv. Matteo Martelli	n. 9
avv. Alessandra Mezzadri	n. 10
avv. Alberto Montanarini	n. 9
avv. prof. Lucia Silvagna	n. 9
avv. Marcello Ziveri	n. 10

Nella sua nuova composizione (2019 – 2022) dal 7 marzo fino al 9 maggio 2019 il Consiglio si è riunito 9 volte.
Elenco delle presenze dei Consiglieri alle adunanze:

Presidente avv. Simona Cocconcelli	n. 9
Consigliere Segretario avv. Daniela Bandini	n. 9
Consigliere Tesoriere: avv. Stefano Squarcina	n. 9
avv. prof. Luigi Angiello	n. 9
avv. Lorenzo Bianchi	n. 9
avv. Angelica Cocconi	n. 8
avv. Fabrizio Ferri	n. 8
avv. Maria Carla Guasti	n. 9
avv. Matteo Mancini	n. 7
avv. Matteo Martelli	n. 7
avv. Francesco Mattioli	n. 9
avv. Michele Megha	n. 9
avv. Fabio Mezzadri	n. 5
avv. Maria Rosaria Nicoletti	n. 9
avv. Alessandra Palumbo	n. 8
avv. Maurizio Paride Donelli	n. 1

(Il Consiglio, nella riunione del 19 marzo 2019, preso atto delle dimissioni dalla carica di consigliere presentate dall'avv. Maurizio Paride Donelli, ha designato quale consigliere subentrante ex art. 16 L. 113/2017 l'avv. Fabio Mezzadri, quale primo iscritto non eletto nell'Assemblea del 26 febbraio 2019).

Nella prima seduta il Consiglio ha formato le Commissioni per il quadriennio di carica.
• Commissione Formazione e Aggiornamento:
avv. prof. Luigi Angiello avv. Daniela Bandini avv. Lorenzo Bianchi avv. Simona Cocconcelli avv. Matteo Mancini avv. Michele Megha vv. Maria Rosaria Nicoletti avv. Alessadra Palumbo

• Commissione Pratica Forense anche per il Progetto di Alternanza Scuola Lavoro:
avv. Angelica Cocconi avv. Maria Carla Guasti avv. Michele Megha avv. Fabio Mezzadri
avv. Maria Rosaria Nicoletti

• Commissione Rapporti con la Magistratura:
avv. Simona Cocconcelli avv. Fabrizio Ferri avv. Maria Carla Guasti avv. Matteo Martelli avv. Francesco Mattioli avv. Michele Megha avv. Alessadra Palumbo

• Commissione Parcelle:
avv. Angelica Cocconi avv. Matteo Mancini avv. Francesco Mattioli avv. Michele Megha avv. Fabio Mezzadri avv. Maria Rosaria Nicoletti

• Commissione Informatica:
componenti interni: avv. Lorenzo Bianchi avv. Stefano Squarcina
componenti esterni: avv. Marina Cafferata avv. Vincenzo Ciriello avv. Matteo de Sensi avv. Luigi Martin avv. Tommaso Zamboni

• Commissione Regolamenti:
avv. Matteo Martelli avv. prof. Luigi Angiello

• Commissione Difese d'ufficio :
avv. Maria Rosaria Nicoletti avv. Francesco Mattioli

• Commissione Patrocinio a spese dello Stato:
avv. Daniela Bandini avv. Maria Carla Guasti avv. Alessandra Palumbo

• Commissione redazione di Cronache dal Foro Parmense
componenti interni: avv. prof. Luigi Angiello avv. Simona Cocconcelli avv. Angelica Cocconi avv. Matteo Mancini
componenti esterni: avv. Nicola Bianchi avv. Alberto Magnani

• Commissione Sovraindebitamento:
avv. Lorenzo Bianchi avv. Simona Cocconcelli avv. Fabrizio Ferri avv. Matteo Martelli avv. Giuseppe Bruno (esterno)

• Commissione Protocollo Diritto Famiglia:
avv. Daniela Bandini avv. Maria Carla Guasti avv. Matteo Mancini avv. Alessandra Palumbo

• Commissione sulle procedure arbitrali:
avv. prof. Luigi Angiello avv. Lorenzo Bianchi avv. Simona Cocconcelli avv. Fabrizio Ferri

• Componenti Organismo di Mediaconciliazione:
avv. Enrico Maggiorelli (Responsabile esterno) avv. Stefano Squarcina (Consigliere Responsabile) avv. Daria Fanti

Comitato Pari Opportunità (CPO) per il biennio 2019/2020:
avv. Angelica Cocconi (referente Consiglio) avv. Alessandra Palumbo (referente Consiglio)
avv. Cecilia Cortesi Venturini (eletta)
avv. Cristina Costantino (eletta)
avv. Gianmarco Di Giuseppe (eletto)

OPINAMENTO PARCELLE

Dal 22 novembre 2018 al 9 maggio 2019 l'apposita commissione consiliare (ovvero il Consiglio) ha espresso n. 68 pareri di congruità e n. 1 opinamento.

Tentativi di conciliazione ai sensi dell'art. 13 L. 247/2012 dal 22 novembre 2018 al 9 maggio 2019:
- riusciti n. 2
- non riusciti n. 5
- non tenuti n. 2

ESPOSTI

Dal registro dei reclami nei confronti degli iscritti dal 22 novembre 2018 al 9 maggio 2019:
- Pervenuti n. 43, tutti trasmessi al CDD di Bologna.

RICHIESTE DI AMMISSIONE AL PATROCINIO DELLO STATO

Decisioni delle delibere consiliari dal 22 novembre 2018 al 9 maggio 2019:
istanze pervenute n. 160 di cui:
ammesse n. 140;
ammesse con riserva n. 3;
non ammesse n 1;
in sospeso n. 16;
revocate n. 6.

Aggiornamento Albi

ISCRIZIONI

BARBARA BISASCHI (28 novembre 2018);
ROCCO MEZZATESTA (18 dicembre 2018);
MATTEO BRIZZI (9 gennaio 2019);
GIULIA SPAGNOLO (9 gennaio 2019);
ANGELA LO RUSSO (9 gennaio 2019);
GIULIA VEZZONI (9 gennaio 2019);
EMANUELA MAIO (9 gennaio 2019);
KARIMA TASSA (9 gennaio 2019);
EUGENIA BONAPACE (9 gennaio 2019);
MICHELE TAGLIAVINI (9 gennaio 2019);
ANNUNZIATA FLAGIELLO (9 gennaio 2019);
PAOLO LAZZARI (17 gennaio 2019);
FRANCESCA MARROLLO (17 gennaio 2019);
DANIELA MARRAZZO (reiscrizione, 17 gennaio 2019);
CRISTIANO COSTANTINO LODDO (29 gennaio 2019);
MARIA IARIA (reiscrizione all'Elenco speciale degli avvocati addetti ad Uffici Legali, 5 febbraio 2019);
ANNABELLA ALFIERI (20 febbraio 2019);
GIACOMO COMPIANI (12 marzo 2019);
ALESSANDRA ABBATE (16 aprile2019)
CRISTIANO COSTANTINO LODDO (dall'albo ordinario all'Elenco speciale degli avvocati addetti ad Uffici Legali, 16 aprile 2019)
MATTIA DE PASCALE (7 maggio 2019)

CANCELLAZIONI

ARISTIDE SPANO' (a domanda, 28 novembre 2018);
GIUSEPPE ABRATI (a domanda, 28 novembre con decorrenza 31 dicembre 2018);
RODOLFO CAPUTO (a domanda, 4 dicembre 2018);
FRANCESCA ILLICA MAGRINI (a domanda, 11 dicembre 2018);
LORENZO BELTRAME (a domanda, 11 dicembre 2018);
GIOVANNI MALMESI (a domanda, 18 dicembre 2018);
PAOLO RABAIOTTI (a domanda, 9 gennaio 2019);
MARCELLO D'ANTONANGELO (12 marzo 2019, per decesso avvenuto il 26 febbraio 2019);
LUIGI LEVORI (per trasferimento all'ordine di Brescia; delibera 19 marzo con decorrenza 11 marzo 2019);
MICHELE BOGGIANI (a domanda, 26 marzo 2019);
ANGELA LILIANA FALCIANO (per trasferimento all'ordine di Reggio Emilia; delibera 7 maggio 2019)

alla data del 7 maggio 2019 gli iscritti all'albo erano **milleduecentosettantatre**

PRATICANTI AVVOCATI

Iscritti	n. 30
Cancellati	n. 46

PRATICANTI AVVOCATI -tirocinio anticipato ex art. 41 c. 6 lett. d) legge 247/2012-

Iscritti	n. 3

PATROCINATORI LEGALI

Iscritti	n. /
Cancellati	n. 11

PRATICANTI ABILITATI AL PATROCINIO SOSTITUTIVO

Iscritti	n. 7
Cancellati	n. /

Variazioni

avv. LORENZA SQUERI: Parma, viale Tanara n. 9, invariati gli altri dati;

avv. LAURA PASSERETTI: Parma, via Enrico Sartori n. 26, tel. e telefax 0521/939144, e-mail avvpasseretti@studiopasseretti.it, posta elettronica certificata avvpasseretti@pec.studiopasseretti.it;

avv. PIETRO FRANCHI: tel. e telefax 0524/522445;

avv. ANGELA LO RUSSO: e-mail avv.lorusso-angela@gmail.com;

avv. FRANCESCA PAGLIARI: telefax 0521/522253 invariati gli altri dati;

avv. CRISTINA MONTANINI: tel. 0521/620519 e telefax 0521/621036;

avv. GIULIA CUCCHI: Parma, via F. Petrarca n. 9;

avv. MARIO CLAUDIO CAMMARATA: telefax 0521/522253, invariati gli altri dati;

avv. MANUELA FRIGGERI: telefax 0521/1621507, e-mail m.friggeri@afstudio-legale.com;

STUDI LEGALI ASSOCIATI: "Studio Legale Associato Caravà – Cavalli" studio legale associato cessato;

STUDI LEGALI ASSOCIATI: "Studio Legale e Tributario Caffarra e Associati" composto dall'avv. Luigi Caffarra e dall'avv. Cinzia Magri;

STUDI LEGALI ASSOCIATI: "Studio Legale Associato Varalla & Musio" studio legale associato cessato;

avv. POMPEO GIOVANNI MUSIO: tel. 0521/389903 non attivo, e-mail avv.musio@studiomusio.it;

avv. CONCETTA ANNA VARALLA: tel. 0521/386611 non attivo;

avv. MARIA PIA PELLEGRINO: tel. 0521/208847 (unica utenza), cell. 338/1544044;

avv. FILIPPO MATTIOLI: Parma, stradello Marche n. 6, invariati gli altri dati;

avv. RAFFAELLA AZZALI: telefax 0521/1621507, e-mail r.azzali@afstudiole-gale.com;

avv. EMANUELA DI NALLO: e-mail dinallo@lexstudio.eu;

avv. MARCELLO GIANINI: e-mail marcello-gianini69@gmail.com;

avv. UMBERTO SERRA: Parma, borgo Guazzo n. 42, cell. 370/3490217, telefax 0521/237704, e-mail umberto.serra@avvo-catoserra.com;

STUDI LEGALI ASSOCIATI: "Serra Landini De Rosa Studio legale tributario" varia la denominazione in "Landini De Rosa Studio legale tributario";

avv. SARA SEGANTINI: Parma, stradello Marche n. 6, tel. 0521/237578, telefax 0521/236840, e-mail s.segantini@studio-furlotti.it;

avv. FRANCESCO SAGGIORO: Parma, viale V. Bottego n. 3, cell. 347/7708196, invariati gli altri dati;

avv. MARIA LUCIA DELLAPINA: posta elettronica certificata avvocatodellapina@arubapec.it;

avv. LUIGIA CASTIGLIEGO: e-mail avv.luigiacastigliego@hotmail.it, posta elettronica certificata avv.luigiacastigliego@legalmail.it;

avv. RAFFAELE BUSANI: Salsomaggiore Terme, via Divisione Julia n. 1, cell. 328/2781320, invariati gli altri dati;

avv. VALENTINA MIGLIARDI: Parma, borgo Santa Chiara D'Assisi n. 8, invariati gli altri dati;

STUDI LEGALI ASSOCIATI: "Studio Legale Associato Boselli – Del Fante – Montanini" studio legale associato cessato;

avv. ANNA PAPADIA: Parma, borgo Santa Chiara D'Assisi n. 8, invariati gli altri dati;

avv. GIUSEPPE TRICARICO: e-mail avv.giuseppetricarico@virgilio.it, posta elettronica certificata avv.giuseppetricarico@legalmail.it;

avv. CRISTIANO OSTI: e-mail studiolegale@cristianoosti.it;

avv. MARA MENATTI: Parma, via Enrico Sartori n. 26, tel. e telefax 0521/939144;

avv. ANNA LEDA GRECO: e-mail annaleda@grecolegal.com, posta elettronica certificata annaleda.greco@pec.it;

avv. LAURA CAVANDOLI: Parma, via Giuseppe Verdi n.21, e-mail avv.lauracavandoli@gmail.com;

avv. SIMONE ALBERICI: e-mail studiolegale-alberici@gmail.com;

avv. BARBARA UGOLOTTI: Parma, borgo Felino n. 29, tel. 0521/282210, telefax 0521/208515, e-mail barbara.ugolotti@avvocatiscotti.it;

avv. SABRINA MARINA SPAGNOLI: Parma, borgo Ronchini n. 9, invariati gli altri dati;

dott. DAVIDE CATTABIANI: Parma, borgo Giacomo Tommasini n. 18, tel. 0521/1851805, cell. 348/7852452, invariate e-mail e posta elettronica certificata;

avv. ESTER TORSELLO: Parma, via Farini n. 20, tel. 0521/200055, telefax 0521/284560;

avv. FABRIZIO MONTANINI: tel. e telefax 0524/332335;

avv. ALBERTO DE DOMINICIS: tel. e telefax 0521/570360;

avv. MARINA CAFARO: telefax 0521/1622220;

avv. SIMONA PESCHIERA: Parma, via Massimo D'Azeglio n. 23, invariati gli altri dati;

avv. FRANCESCO SANSONE: Parma, galleria Polidoro n. 8, e-mail avvfrancescosansone@gmail.com, invariati gli altri dati;

avv. ENRICO MAGGIORELLI: telefax 0521/200203;

avv. ANTONINO TUZI: tel. non attivo, cell. 328/9792525, telefax 0521/1731704;

avv. STEFANIA LAMBERTI ZANARDI: Parma, strada della Repubblica n. 64, tel. 0521/774991, cell. 347/2721002, telefax 0521/778681, invariati gli altri dati;

avv. ROBERTA ROLLO: telefax 0521/204045;

avv. VALENTINA VITELLI: telefax 0521/1474042;

avv. ILIUSKA DE NUZZO: e-mail avv.denuzzo@gmail.com;

avv. MARIO L'INSALATA: e-mail mario@studiolegalelinsalata.it;

avv. CRISTIANO CIMADOM: unico tel. attivo 0521/506607;

avv. BEATRICE MENZANI: tel. 0521/571796, sito internet www.menzani.it, invariati gli altri dati;

avv. VINCENZO ZICCARDI: unico tel. attivo 0521/508737;

avv. VALENTINA TUCCARI: e-mail vtuccari@studiolegaletuccari.it;

avv. BENEDETTA CODELUPPI: Parma, piazzale Boito n.1, tel. 0521/1412018, 0521/283122, invariati gli altri dati;

avv. LORENZO PAOLO BOTTI: posta elettronica certificata lorenzobotti@pec.giuffre.it;

avv. FEDERICA PIOMBI: telefax 0521/1474042;

avv. SIMONE GABBI: posta elettronica certificata simone.gabbi@pec-legal.it;

avv. CARLOTTA DEL MONTE: Parma, via Fra Salimbene da Parma n. 12, tel. 0521/200035, telefax 0521/1852698, e-mail carlottadelmonte83@gmail.com, invariata la posta elettronica certificata;

avv. TOMMASO MARIO ORRU': e-mail avvtommasomariorru@libero.it;

avv. MICHELANGELO LANZI: casella UNEP n. 387;

avv. SEBASTIANO GUERZONI: casella UNEP n. 387;

avv. CHIARA LAEZZA: Parma, strada Giuseppe Garibaldi n. 22, tel. 0521/285625, telefax 0521/1622130, cell. 329/8720954, invariati gli altri dati;

avv. GIUSEPPINA ZENNA: telefax 0521/883252;

avv. ANGELICA COCCONI: telefax 0521/883252;

avv. PAOLA MAGGIORELLI: tel. e telefax 0521/235810, cell. 348/8891146;

avv. FABIO APOLLONIO: e-mail avv.apollonio@gmail.com;

avv. GIOVANNI NOUVENNE: telefax 0521/883252;

avv. GIORGIO FERRARI: e-mail studiolegalegiorgioferrari@gmail.com;

avv. VIVIANA SCARAMUZZINO: Parma, via Pecchioni n. 10, tel. 0521/499131, tel. e telefax 0521/243270, invariati gli altri dati;

avv. VALENTINA CIURLEO: Parma, vicolo dei Mulini n. 4, telefax 0521/711258, invariati gli altri dati;

avv. ALESSANDRO TELLINI: posta elettronica certificata a.tellini@postecert.it;

avv. RENATO DEL CHICCA: Parma, borgo Cantelli n. 7, cell. 340/8087349, invariate e-mail e posta elettronica certificata;

avv. MICHELE DE LUCA: e-mail michele.deluca.parma@gmail.com;

avv. MATTEO BRIZZI: cell. 351/8881766; e-mail avvmatteobrizzi@gmail.com;

avv. SILVIA CARAVA': tel. 0521/241467, telefax 0521/1811984;

avv. LETIZIA CAVALLI: Parma, borgo del Parmigianino n. 16, invariati gli altri dati;

avv. PAOLA MARENZONI: secondo studio Langhirano, piazza Garibaldi n. 16, cell. 347/0922841, invariati gli altri dati;

avv. CARLO ABLONDI: e-mail carlo@lablawyers.cloud;

avv. ANDREA SIMONAZZI: tel. 0521/1522121, telefax 0521/1854560, cell. 335/7230659;

avv. BERNARDO ROGNETTA: Parma, via Emilia Est n. 16, tel. fisso non più attivo, cell. 327/7084707, telefax 0521/1815481, ;

avv. ANNAMARIA D'AMONE: telefax 0521/1550276, cell 347/7627712;

avv. BARBARA BISASCHI: Montechiarugolo (PR) via G. Matteotti n. 1/B, cell. 348/3354215;

avv. FRANCESCA ANGHINOLFI: e-mail francesca.anghinolfi@agenziapo.it;

avv. FRANCESCA POLETTI: cell.338/9924109, tel. fisso e telefax non più attivi;

avv. ALESSANDRA FRASSINETTI: e-mail afrassinetti@units.it;

avv. SIMONA FERRARI: tel. e telefax 0521/883656;

avv. SILVANO CARUCCIO: Parma, via Mazzini n. 43, tel. e telefax 0521/677414, e-mail silvanocaruccio@libero.it;

avv. CRISTIANO AIMI: Fontanellato (PR), via Roma n. 14, invariati gli altri dati;

avv. ARIANNA IMBRIANI: secondo studio in San Secondo Parmense, piazza Martiri della Libertà n. 10;

avv. MARIANGELA CASTELLANA: Parma, viale Partigiani d'Italia n. 8/1, tel. 0521/244005, telefax 0521/389902, e-mail castellana.mariangel@libero.it, posta elettronica certificata avv.castellana@pec.it; domicilio professionale presso avv. Massimo Ferrari (e-mail m.ferrari@avvocatiferraritanzi, posta elettronica certificata avvmassimoferrari@pec.it);

avv. VIVIANA MANTIONE: tel. 0521/240304, cell.371/3266852, invariati gli altri dati;

avv. ANNA ADELE CARAFFINI: fax non più attivo;

avv. MATTIA AMBANELLI: fax non più attivo;

avv. GIANLUIGI MATTEO REGISTRO: Parma, strada G. Mazzini n. 43, tel. e telefax 0521/677141;

Mozione congressuale "Per l'effettività della tutela dei diritti e la salvaguardia della giurisdizione"

L'Avvocatura Italiana, nella sessione ordinaria del XXXIV Congresso Nazionale Forense di Catania, ha già indicato la necessità di un rafforzamento della salvaguardia della autonomia e indipendenza dell'Avvocatura, quale garanzia della effettività della tutela giurisdizionale dei diritti e presidio di libertà e democrazia.

Questa affermazione si fonda sulla consapevolezza che l'attività dell'Avvocato si estrinseca, prima di tutto, all'interno della giurisdizione per la concreta tutela ed attuazione dei diritti, costituzionalmente garantiti, dei cittadini e della società civile. Tutte le altre importanti funzioni svolte dall'Avvocato, comprese quelle esercitate nelle modalità alternative di risoluzione delle controversie, pur quando si articolano al di fuori della giurisdizione si fondano perciò sul ruolo dell'Avvocato di *"garante della tutela giurisdizionale dei diritti"*.

Poste queste premesse e nella consapevolezza delle responsabilità che tale ruolo le attribuisce, l'Avvocatura Italiana avverte la necessità di denunciare che la Giurisdizione sta subendo da molti anni un lento ma progressivo deterioramento, sia riguardo alla sua capacità di offrire tempestiva e concreta tutela ai diritti violati, sia riguardo alla perdita di credibilità e legittimazione che ha ricevuto nei confronti della società civile italiana.

I segnali di crisi sono chiaramente manifestati, in primo luogo, dalla abnorme durata dei tempi di risposta alle domande di giustizia dovuti principalmente alla assoluta inadeguatezza delle risorse umane e materiali che le sono destinate: tale problema non può essere risolto riducendo gli spazi di difesa e del contradditorio, come emerge dall'uso improprio e a fini dissuasivi di strumenti preclusivi, come le inammissibilità e le sanzioni processuali e l'aumento ingiustificato dei costi di accesso, ma riaffermando il principio per cui l'efficienza e l'efficacia della Giurisdizione non possano essere valutate con riferimento a criteri meramente "economistici" e "aziendalistici" e debbano invece essere commisurate all'adeguatezza e certezza della tutela dei diritti che essa sia in grado di assicurare in modo concreto ed effettivo.

La garanzia di una adeguata tutela dei diritti è poi messa in crisi dall'impiego indiscriminato di magistrati onorari e dall'allargamento delle competenze dei Giudici onorari di prossimità, senza garanzie generali di professionalità, competenza e terzietà, che svilisce la funzione e la credibilità della Giurisdizione e le impedisce di assicurare uniformità all'interpretazione dell'Ordinamento Giuridico e certezza ai rapporti sociali.

Va inoltre segnalato il concreto pericolo che la Giurisdizione, da funzione primaria dello Stato volta alla tutela dei diritti lesi, divenga esercizio di potere, come rischia di avvenire nel caso della giustizia repressiva penale o contabile, o semplice servizio pubblico, come avviene invece per la giustizia civile, amministrativa e tributaria.

Il giustizialismo, quale "reazione" alla fragilità delle istituzioni e alla vulnerabilità del corpo sociale, con la richiesta di sanzioni "esemplari" e la deriva del linguaggio d'odio, ha fatto sì che da anni l'azione di repressione dei reati stia svolgendo un ruolo di supplenza alla debolezza delle azioni politiche ed amministrative. Tale fenomeno, causa dell'inaccettabile spettacolarizzazione della repressione penale quale risposta alla esigenza di sicurezza sociale, indica con chiarezza

CONGRESSO NAZIONALE FORENSE

ROMA
5-6 APRILE 2019

il rischio di una deriva retriva ed illiberale in cui la sempre maggiore richiesta di sanzione giustizialista incentivi una progressiva e pesante contrazione delle prerogative difensive processuali dell'imputato: dovendosi sempre rammentare che un imputato innocente condannato per carenza di garanzie, oltre a dar luogo ad un inaccettabile disvalore etico e di civiltà, è comunque una grave sconfitta anche per la società civile quando resti impunito l'effettivo autore del reato.

L'esigenza di rafforzare le garanzie della difesa si avverte in modo sempre più pressante anche con riguardo alla Giurisdizione contabile, dove l'azione risarcitoria e sanzionatoria dello Stato viene svolta in condizioni di inadeguata garanzia per i diritti delle parti private.

Ma il rischio di deriva illiberale della nostra giurisdizione si coglie anche, su un piano più generale, *nell'irrigidimento potrebbe aggravarsi ove l'irrigidimento e nellala riduzione degli strumenti di interpretazione offerti per la interpretazionel'interpretazione evolutiva del nostro ordinamento giuridico per effetto della, conseguenti alla affermazione didei principi* nomofilattici che, introdotti con riferimento alle decisioni a sezioni unite della Corte di Cassazione ed in corso di recepimento anche nelle altre sedi giurisdizionali, sono potenzialmente idonei ad impedire l'adeguamento dinamico, non fosse contemperato dalla salvaguardia del sistema delle tutele dei diritti all'evoluzione sociale e tecnologica, se non si salvaguarderà il principio del *"libero convincimento" del giudicee la liberaGiudice e dalla predisposizione di adeguate garanzie per la possibilità delle parti di prospettare interpretazioni dell'ordinamentogiuridiche diverse da quelle già affermate dalla giurisprudenza, purché non mosse da intenti pretestuosi*.[1]

Sotto altro profilo, la tutela giurisdizionale è sempre più assimilata, nel linguaggio corrente e nel comune sentire, ad un mero "servizio", al pari di altri servizi di natura amministrativa*, cosicché si profila con il rischio che*[1] intere branche di giurisdizione possano essere demandate a plessi di "giurisdizione privata". Con l'ulteriore rischio che, definita la giurisdizione in tali termini di servizio e acclarata la inefficienza dell'organizzazione giudiziaria da parte dello Stato, si aprano sempre maggiori spazi alla gestione in forma economica del servizio di risoluzione dei conflitti e delle incertezze interpretative dell'Ordinamento Giuridico.

La questione si pone con particolare urgenza e gravità nel campo del diritto civile, dove la giurisdizione, per il modo in cui viene esercitata, fa fatica a svolgere il proprio ruolo di composizione dei conflitti economici e sociali.

Si ha riguardo, certamente, alle conseguenze del gravissimo ritardo della risposta del Giudice civile nella regolazione dei rapporti economici, con particolare riferimento agli operatori economici e sociali di piccole e medie dimensioni e alle distorsioni di sistema che ne conseguono; ma non minore attenzione merita la tendenza, sempre più accentuata, a sottrarre alla sfera e alla volontà delle parti la disponibilità dei diritti fatti valere in giudizio, con il rischio del progressivo scivolamento verso un processo autoritario e snaturato nella sua essenza.

Tale fenomeno inizia a manifestarsi, del resto, anche sul piano della adeguatezza della giurisdizione a dare composizione ai conflitti sociali, come nel campo del diritto di famiglia, e in tutti i casi in cui la Giurisdizione è chiamata a dare tutela e supporto alle situazioni di disagio sociale.

Ancor più delicato e rilevante appare il ruolo della Giurisdizione per la tutela dei cittadini e delle imprese avverso gli atti autoritari di esercizio del potere amministrativo. Si tratta di un plesso di giurisdizione che richiede interventi per rafforzare l'effettività della risposta giurisdizionale alle esigenze della nostra società.

Sull'efficacia della tutela giurisdizionale amministrativa grava inoltre la ridotta sindacabilità degli atti delle "autorità amministrative indipendenti", nei cui confronti il sindacato giurisdizionale viene spesso ritenuto come "debole".

Infine, l'efficacia della tutela dei diritti in materia amministrativa è in molti casi fortemente ridotta dagli abnormi costi di accesso, che determinano un distorsivo effetto di dissuasione e riducono in modo gravissimo la concreta possibilità di accesso alla Giurisdizione.

Analoghe considerazioni vanno svolte rispetto alla strutturale inadeguatezza del sistema di tutela tributaria, che ancora non è dotato di un giudice totalmente terzo e adeguatamente professionalizzato e specializzato.

Riguardo ai rischi così paventati, l'Avvocatura Italiana, nel proprio ruolo di garante della tutela dei diritti in generale, approva il seguente

DELIBERATO

L'Avvocatura Italiana, riunita in sessione ulteriore del Congresso Nazionale Forense a Roma il giorno 6 aprile 2019,

RIAFFERMA

quale imprescindibile principio di democrazia e civiltà, la centralità della Giurisdizione quale funzione primaria resa dallo Stato in condizioni di terzietà per la tutela dei diritti dei cittadini e della collettività al fine della concreta realizzazione dei valori costituzionali di libertà e uguaglianza sostanziale

CHIEDE

a tal fine, che

- siano destinate alla Giurisdizione risorse adeguate al ruolo che la Costituzione le attribuisce, al fine di garantire l'effettiva realizzazione dei diritti degli individui, della collettività e del sistema produttivo del Paese, sia riservandole l'intero gettito derivante dalle imposte specificamente afferenti alla "Giustizia" sia attribuendole le ulteriori risorse necessarie a carico della fiscalità generale;

- si pongano in essere urgenti interventi affinché la "funzione giurisdizionale" si svolga con regole improntate ai canoni costituzionali del "giusto processo", nel pieno ed effettivo contraddittorio tra le parti in condizioni di parità, davanti ad un giudice sempre terzo, imparzia-

1 il Vostro redattore è ben consapevole che in questa frase (e nelle altre due riportate in carattere corsivo) molto non corre e qualcosa manca, ma è quanto pubblicato sul sito specifico (e sembrerebbe fotocopia dell'originale mozione congressuale); richieste di chiarimento rivolte all'organismo congressuale forense OCF e, su indicazione di questo, al Consiglio nazionale forense CNF ed ancora all'OCF, di ritorno, non hanno avuto esito, nonostante plurimi solleciti il che non depone bene per i nostri organismi rappresentativi data l'importanza politica del proclama.

le e professionale, entro una durata "ragionevole";

- sia sempre garantito il pieno e libero esercizio del diritto delle parti a svolgere adeguata difesa tecnica;

- l'efficienza e l'efficacia della Giurisdizione siano commisurate alla adeguatezza e certezza della tutela dei diritti che essa sia in grado di assicurare in modo concreto ed effettivo mediante il soddisfacimento dell'interesse sostanziale leso;

- l'accesso alla Giurisdizione sia assicurato a tutti, senza preclusioni di censo e senza che l'entità dei costi di accesso alla Giustizia costituisca elemento dissuasivo.

IMPEGNA

l'Organismo Congressuale Forense e tutte le componenti dell'Avvocatura a perseguire fermamente i principi affermati con il seguente

Manifesto dell'avvocatura italiana Per l'effettività della tutela dei diritti e per la salvaguardia della Giurisdizione

1) La Giurisdizione va salvaguardata e potenziata quale *"funzione primaria dello Stato"* costituzionalmente posta per la concreta ed effettiva realizzazione dei diritti dei singoli, della collettività e del sistema produttivo del Paese, al fine della concreta realizzazione dei valori costituzionali di libertà e uguaglianza sostanziale e assicurando le esigenze di certezza nei rapporti sociali ed economici

2) La Giurisdizione deve assicurare il soddisfacimento dell'interesse leso

3) La funzione giurisdizionale deve essere svolta sempre e in ogni caso da parte di un *"Giudice terzo imparziale e professionale"*

4) L'accesso alla Giurisdizione deve essere assicurato a tutti, senza discriminazioni di censo e senza che l'entità dei costi costituisca elemento dissuasivo

5) La Giurisdizione deve essere sostenuta, in attuazione dei principi di solidarismo costituzionale, con risorse materiali e umane adeguate al ruolo assegnatole dalla Costituzione Italiana riservandole, oltre al gettito derivante dalle imposte specificamente afferenti alla "Giustizia", le ulteriori risorse necessarie da porre a carico della fiscalità generale

6) La Giurisdizione si attua mediante le regole e i principi costituzionali del *"giusto processo",* nel pieno ed effettivo contraddittorio tra le parti in condizioni di parità, davanti ad un giudice sempre *"terzo, imparziale e professionale",* entro una durata *"concretamente ragionevole"*

7) La garanzia di autonomia e indipendenza dell'Avvocato e di tutti i soggetti che concorrono all'esercizio della Giurisdizione sono strumento di effettività della tutela dei diritti e presidio di democrazia

8) La presenza di esponenti dell'Avvocatura negli organi di governo dell'istituzione giudiziaria e il rispetto dell'Avvocato nell'esercizio della giurisdizione costituiscono garanzia di una *"efficace e buona Giurisdizione"*

9) La concreta tutela giurisdizionale dei diritti presuppone la piena parità delle parti nel processo e la effettiva esplicazione del diritto di difesa, mediante una adeguata difesa tecnica resa da un Avvocato in condizioni di autonomia ed indipendenza

10) Il principio di non colpevolezza nel processo penale è imprescindibile garanzia di giustizia sia per l'imputato che per la collettività

11) Il rafforzamento del valore interpretativo del precedente giurisprudenziale secondo i principi della cd. "nomofilachia" è strettamente funzionale alle esigenze di certezza giuridica nei rapporti sociali, ma deve avvenire nel costante e imprescindibile rispetto del canone del *"libero convincimento"* del Giudice e garantendo la libera possibilità delle parti di prospettare interpretazioni giuridiche diverse da quelle già affermate dalla giurisprudenza, purché non mosse da intenti pretestuosi, al fine dell'adeguamento dinamico dell'Ordinamento Giuridico

12) Deve essere sempre garantita la piena ed effettiva tutela giurisdizionale nei confronti degli atti e dei comportamenti espressione del potere pubblico

Segnali di fumo

il diritto preso sul serio & il diritto preso sul ridere*

"Bisogna distinguere i ladri.
C'è il ladro ingenuo che porta via i portafogli
dalla tasca della vittima e finisce in prigione,
c'è il ladro abile, intellettuale,
che specula e arricchisce con danno altrui,
con la miseria altrui;
la nostra società non lo chiama ladro,
lo chiama magari commendatore"
(Luglio 1922: dall'arringa dell'Avv. Gustavo Ghidini a favore del Prof. Aurelio Candian nel processo Candian -Lusignani)

La soffitta del diritto.

I gatti di campagna sono soliti portare in bocca i topi acchiappati ed esibirli orgogliosamente al loro padrone. Ma il nostro è un gatto di biblioteca, ed ha eseguito a perfezione la ricerca che gli ho affidato. Trascina a fatica la rivista la cui copertina compare qui sotto.


IL FORO ITALIANO
RACCOLTA GENERALE
DI
GIURISPRUDENZA CIVILE, COMMERCIALE, PENALE, AMMINISTRATIVA
DIRETTORI
DE CRESCENZO
MUCACCI
SCIALOJA
VOLUME I – ANNO 1876
ROMA
IL FORO ITALIANO
TIPOGRAFIA EREDI BOTTA
1877

Si tratta del primo, primissimo numero di Foro Italiano, anno 1876.

Il percorso formativo dei nostri colleghi antenati (IV)

Gli avvocati antifascisti e resistenti nel parmense

Piero Calamandrei già all'indomani della destituzione di Mussolini sostenne che gli avvocati sinceramente devoti al fascismo erano stati pochi: "*di tutti gli Ordini professionali, quello che ha più sofferto nel profondo l'oltraggio di questa goffa e umiliante tirannia durata vent'anni, è stato il nostro, l'Ordine degli Avvocati: perché noi a differenza di tante altre professioni, non abbiamo mai trovato nel nostro quotidiano lavoro il pretesto per distrarci dalla realtà politica che ci attorniava e per rasserenarci in altri cieli (...) ma abbiamo incontrato ogni giorno, anzi dieci volte al giorno, nel maneggio delle leggi che costituisce la nostra quotidiana fatica, la conferma esasperante della nostra vergogna (...) specialmente negli anni immediatamente seguenti all'avvento del "regime", l'esercizio del patrocinio forense è stato un duro tirocinio di coraggio civile e di abnegazione spinta tal volta fino al sacrificio della vita".*[1]
Concetti ribaditi nel febbraio 1945: il fascismo *"odiò sempre sordamente come nemici" gli avvocati – e ancora nel 1947, quando alla vigilia del primo congresso forense "dell'Italia Libera" di Firenze intese commemorare quanti "hanno preferito il sacrificio alla viltà, ed hanno con questo testimoniato che la giustizia, al servizio della quale è la nostra professione, è un impegno grave e solenne, che vale per la vita e per la morte".* Molti, del resto, gli avvocati tra le decine di migliaia di italiani che, tra il settembre '43 e il maggio '45, erano riparati in Canton Ticino, ricercati e perseguitati per motivi politici o razziali (ebrei, oltre a soldati sbandati, renitenti alla leva fascista, partigiani) che avevano fatto questa scelta estrema per evitare il confino o la deportazione. [2] Questa atmosfera anti libertaria sia acuisce quando il fascismo, superato il grave trauma del delitto Matteotti, entrò nella fase del consenso e della "normalizzazione".

1 P. Calamandrei "*gli avvocati e la libertà*".


AVV.
GIUSEPPE BARBIERI
14·2·1908 – 1·9·1944
TEMPRA PURISSIMA DI COSPIRATORE E DI COMBATTENTE
IMPAVIDO FRA ATROCI SEVIZIE
FU TRUCIDATO IN PIAZZA GARIBALDI
DAI RINNEGATI ASSERVITI AL TEDESCO
AVV.
ARNALDO CANALI
23·4·1894 – 16·11·1944
AVV.
AUGUSTO OLIVIERI
4·5·1891 – 30·4·1945
LA TOGA NON PIEGARONO ALLA TIRANNIDE
DEPORTATI OLTR'ALPE
DOPO LUNGHI TORMENTI DIEDERO LA VITA
PER LA RINASCITA DEL POPOLO ITALIANO
I COLLEGHI MEMORI

Nell'atrio del nostro Tribunale campeggia questa lapide commemorativa, accanto al busto del Sen. Avv. Gustavo Ghidini, socialista, già Membro della Commissione dei 75 e Presidente della Terza Sottocommissione della Costituente, e già Presidente del nostro Ordine forense.[3]

2 Da Francesca Tacchi *Gli avvocati italiani dall'Unità alla Repubblica*a cura del C.N.F. Ed. Il Mulino.

3 Alla sua scomparsa in Senato fu commemorato con parole di grande affetto dal concittadino sen. PCI Giacomo Ferrari il quale ricordò tra l'altro che fu il "difensore dei poveri"; a nome del PSDI il Sen. Morino: "fu difensore insigne in famosi processi: ad esempio nel 1924, in quello di Aurelio Candian, nel famoso processo Candian – Lusignani. Nel 1944, davanti al Tribunale fascista di Parma, difese l'ammiraglio Enrico Campioni". Il social democratico Lami Starnuti rivolgendosi alla sua famiglia: "ora Gustavino non è più un bambino, e il nonno poteva andare lontano, come è andato per sempre". Oggi quel "Gustavino" è professore ordinario di diritto industriale presso la facoltà di Giurisprudenza della Università Statale di Milano e direttore dell'Osservatorio di proprietà intellet-

*** Quest'ultimo scritto dedico alla mia amatissima moglie Luisella Dalla Chiesa, in particolar modo le pagine su "Il Crepuscolo"**

Augusto Olivieri - padre del nostro collega Gigi scomparso anni fa- venne arrestato nel marzo del 1944 quando aveva 52 anni, insieme al collega Adevaldo Credali. Dopo essere stato recluso in vari carceri, fu destinato al campo di concentramento di Gusen (Austria). Provato dagli stenti e con un braccio fratturato, fu dimesso dalla infermeria per tornare nella baracca comune, ove morì alla vigilia della liberazione, il 28 Aprile 1945, circondato dall'affetto e dalle cure estreme dei compagni internati, che poi scrissero di lui: "è stato per noi tutti un grandissimo dolore la perdita di un così caro compagno, di tanto nobile amico, proprio quando di già assaporava la dolcezza della imminente liberazione".

Augusto Olivieri proveniva da una famiglia di professionisti da sempre legata all'eredità politica risorgimentale. Il padre Erminio, anch'egli avvocato, era stato un fervente radicale, eletto deputato in Parlamento e Sindaco di Parma tra il 1914 e 1919. Contrariamente al padre, Augusto preferì il lavoro alla politica anche se allo scoppio della grande guerra si schierò contro la partecipazione italiana aderendo al movimento anti interventista. Le cose andarono diversamente e con l'ingresso dell'Italia in guerra, Augusto Olivieri, come molti altri giovani italiani che si erano schierati per la neutalità, finì per partire volontario e partecipò "con ardore ed eroismo" (fu anche ferito sul Pasubio) alla prima guerra mondiale.

Fu insignito, a riconoscimento del suo valore, di una medaglia d'argento e di una medaglia di bronzo al valor militare, di una promozione per merito di guerra nonché di una decorazione francese corrispondente alla medaglia d'argento italiana". [4]

L'Avv. Paolo Venturini invece sfuggì all'ordine di cattura che aveva colpito contestualmente i colleghi Olivieri e Credali (il quale sopravvisse).

Non si può tacere il richiamo, nell'ordine di cattura dei due colleghi e nella motivazione al loro essere nel contempo antifascisti e "capi franco muratori".

A prescindere dalla loro attività antifascista si volle colpire la loro appartenenza ad una loggia massonica collegata con il Grande Oriente di Italia (Palazzo Giustiniani), chiusa dal governo Mussolini nel 1925. Il fatto che venissero indicati quali aderenti alla massoneria li collocava politicamente nel campo democratico dell'antifascismo italiano, nell'area liberal socialista che a Parma era stata ed era ancora tutt'altro che marginale nel fronte impegnato nella lotta di liberazione [5]. Questa ascendenza familiare di marca mazziniana – proveniente da una lontana tradizione clandestina in quanto al tempo patriottica – era talvolta comune anche al più alto livello dei comunisti di casa nostra: in questi ultimi in fase di vigile quiescienza fino alle loro ultime volontà. Tale tradizione spesso, non sempre, venne ereditata dalla discendenza che sarà poi attiva nel mondo forense. Del resto, l'aspra contesa che contrappose negli anni '20 Candian e Lusignani vedeva schierate con il primo le logge massoniche di Palazzo Giustiniani, mentre il secondo costituì a Parma la più fascista delle logge di Piazza del Gesù[6]. Non già che la prima resistenza del ceto-medio alto al fascismo avesse per sostanza identitaria solo l'appartenenza a tali appendici dell'associazionismo mazziniano, rappresentava bensì una sorta di *élite* borghese e professionale[7]. Come scrive con proprietà Massimo Giuffredi "Un regime di notabili – il potere a Parma durante il fascismo" DSB Ed. –Centro Studi Movimenti Parma-, pag. 15: "*Nel complesso si trattava non tanto di una classe ma di una formazione sociale identificabile come un ceto, definito, al di là di interessi a volte magari non coincidenti, da un comune stile di vita, da una interna solidarietà nonostante le divergenze. Lo si può per comodità, empiricamente, definire una forma di notabilato (con quel tanto di approssimazione insita nel termine) che, seppure non necessariamente equivalente nel reddito, traeva i propri caratteri da attività professionali, imprenditoriali e culturali quasi sempre unite ad una proprietà di prevalente natura terriera. Con in più, carattere essenziale, la propensione non professionistica alla politica, intesa in primo luogo come gestione del potere locale, a opera di "abbienti istruiti", anche se magari democratici*": caratteristica saliente nella nostra città a differenza di altre limitrofe città emiliane.[8] Radice risorgimentale che si evince dalla stampa qui accanto dell'estratto della sentenza 09.04.1824 di condanna alla pena di morte proferita dal Supremo Tribunale di Revisione del Ducato contro nobili e proprietari terrieri per cospirazione e appartenenza alla Secreta Società dei Sublimi maestri perfetti.

tuale, concorrenza e comunicazione della Luiss Guido Carli.

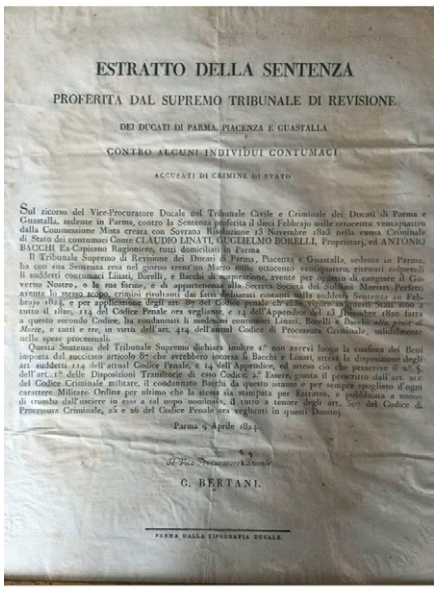
4 R. Lasagni, "*Dizionario biografico dei parmigiani",* P.P.S. Ed. Vol. III°. L'interventismo a Parma fu comune, come noto, tanto ai sindacalisti rivoluzionari, come Alceste De Ambris e Filippo Corridoni –temporalmente accostati al fascismo-, quanto ai notabili – come i sindaci Olivieri e Mariotti-, questi ultimi democratici, massonici e mazziniani, tanto da potersi distinguere nettamente dal fascismo squadrista, limitandone i consensi "sul campo". Esemplarmente Piero Calamandrei, al tempo di osservanza liberale, combattente e decorato nella prima guerra. I "sindacalisti", trascinati dal dannunzianesimo, faticarono a distinguersi dai fascisti combattenti nella guerra. Al punto che nel 1925 Mussolini volle mettere il cappello sull'eroe perito in guerra Filippo Corridoni e ne fece installare, lui presente alla posa della prima pietra, un monumento all'incrocio tra Via Bixio e Via D'Azeglio, donando di sua tasca 1.000 Lire per l'opera. Paradosso parmigiano: nello stesso anno il P.C.I ne rivendicò l'appartenenza intitolandogli una sezione d'Oltretorrente.

5 *Documentare la memoria. La deportazione da Parma* a cura dell'istituto storico della resistenza e dell'età contemporanea / Parma n. 22 pag. 68.

6 L'Avv. Lusignani dopo la contesa con Candian continuò a prendere di mira in particolare gli onorevoli Giuseppe Micheli e Agostino Berenini, con il quale ingaggiò un duello elettorale nel collegio di Fidenza, per lui ostico, uscendone sconfitto per pochi voti. Provocò all'interno del PNF di Parma dissensi e disordini tra fascisti "moderati" e "radicali", rappresentati dal "sulfureo" avvocato conte, con cui il federale avvocato di cui alla nota 17 alternava screzi e alleanze. La federazione fu commissariata nel 1924 dopo che Mussolini, che temeva l'invadenza di Farinacci, aveva inutilmente intimato il 14.02.1924 con questo furibondo telegramma: "*E' ora di finirla con beghe fascismo-parmigiano che ormai non suscitano più nemmeno interesse cronaca minuta (...) fascisti parmigiani la smettano di dare grottesco spettacolo di sé come vanno facendo da ben 5 anni".* Già con telegramma al Prefetto di Parma in data 24.03.1923 Mussolini aveva scritto: "*Episodi insulso illegalismo esautoranti Governo seguiti assassinio fascisti sono sommamente deplorevoli né io intendo passarli sotto silenzio né come Capo Governo né come Capo Fascismo". V.S. chiamerà responsabili dirigenti fascismo locale e 1) esigerà una squalifica dei fascisti che si sono abbandonati a violenze – 2) l'espulsione o la sospensione dal fascio dei responsabili. Se questo non sarà fatto Ella procederà agli arresti secondo le norme non ancora abolite Cod. Penale (Zanardelli, ndr) mentre io scioglierò fascismo parmense. Dica duramente ai signori fascisti che il sangue non si vendica con gesti inutili i quali danneggiano enormemente causa fascista e Nazione".* Evidente l'esigenza di Mussolini, ormai giunto al potere, di assicurare l'ordine pubblico prevenendo i moti della base rissosa, ma, come scrive lo storico De Felice, in "Mussolini e il fascismo" vol. II°, pag. 441, Einaudi 2018, difatto prevarrà l'impunità dei facinorosi.

7 Espressione di questi ceti borghesi democratici negli anni '20 il giornale *Il piccolo*, di cui si è detto a proposito delle barricate: capo redattore Aroldo Lavagetto, padre di Stefano, notaio, sindaco della città per il PDS negli anni 1994 – 1998, il cui figlio e nostro collega, Lorenzo è oggi capogruppo PD nel consiglio comunale. Più risalente *l'idea,* organo dei socialisti riformisti.

8 Tant'è, come osserva il Giuffredi, op. cit. pag. 124, che "dopo la liberazione a differenza di Reggio, Modena, Ferrara e Bologna (ove) si distinguevano nella carica di Sindaco vecchi militanti comunisti di estrazione popolare, a Parma furono sindaci comunisti, dal 1946 al 1951 l'Avv. Savani e il medico e notabile Giuseppe Botteri, di recente adesione al Partito. Forse ancor più significativa risulta la presenza, tra i maggiori e più illustri esponenti del PCI locale, un discendente di un ministro di Maria Luigia, Filippo Magawly, cioè l'Ing. Giacomo Ferrari, comandante delle formazioni partigiane parmensi" che come detto nel testo coprì la carica di Sindaco della città ed altre ancora fino ad essere ministro dei trasporti in due governi De Gasperi.



ESTRATTO DELLA SENTENZA

PROFERITA DAL SUPREMO TRIBUNALE DI REVISIONE

DEI DUCATI DI PARMA, PIACENZA E GUASTALLA

CONTRO ALCUNI INDIVIDUI CONTUMACI

ACCUSATI DI CRIMINE DI STATO

Sul ricorso del Vice-Procuratore Ducale del Tribunale Civile e Criminale dei Ducati di Parma e Guastalla, sedente in Parma, contro la Sentenza proferita il dieci Febbrajo mille ottocento ventiquattro dalla Commessione Mista creata con Sovrana Risoluzione 13 Novembre 1823 nella causa Criminale di Stato dei contumaci Conte CLAUDIO LINATI, GUGLIELMO BORELLI, Proprietarj, ed ANTONIO BACCHI Ex-Capitano Ragioniere, tutti domiciliati in Parma

Il Tribunale Supremo di Revisione dei Ducati di Parma, Piacenza e Guastalla, sedente in Parma, ha con sua Sentenza resa nel giorno trentesimo mille ottocento ventiquattro riuniti sospesovli li suddetti contumaci Linati, Borelli, e Bacchi di comparire, avente per oggetto di cangiare il Governo Nostro, o le sue forme, e di appartenere alla Società Segreta dei Sedicini Massari Perfetti avente lo stesso scopo, crimini risultanti dai fatti dichiarati constanti nella suddetta Sentenza 10 Febbrajo 1824, e per applicazione degli art. 29 del Codice penale ch'era vigente in questi Stati sino a tutto il 1820, 114 del Codice Penale ora vigente, e 14 dell'Appendice del 13 Dicembre 1820 fatta a questo secondo Codice, ha condannati li medesimi contumaci Linati, Borelli e Bacchi alla pena di Morte, e tutti e tre, in virtù dell'art. 414 dell'attual Codice di Procedura Criminale, solidalmente nelle spese processuali.

Questa Sentenza del Tribunale Supremo dichiara inoltre 1° non avervi luogo la confisca dei Beni imposta dal succitato articolo 8° che avrebbero sofferta li Bacchi e Linati, attesa la disposizione degli art. suddetti, 414 dell'attual Codice Penale, e 14 dell'Appendice, ed attesa così che prescrive il n.° 5 dell'art. 12° delle Disposizioni Transitorie di esso Codice 2° Essere, giusta il prescritto dall'art. 2° del Codice Criminale militare, il condannato Pazzia da questo istante e per sempre spogliato di ogni carattere Militare. Ordina per ultimo che la stessa sia stampata per Estratto, e pubblicata a suono di tromba dall'usciere in caso a tal uopo nominato, il tutto a tenore degli art. 507 del Codice di Procedura Criminale, 25 e 26 del Codice Penale ora vegliami in questi Domini.

Parma 9 Aprile 1824.

G. BERTANI.

PARMA DALLA TIPOGRAFIA DUCALE.

Esecutori in genere i popolani, come nel 1854, quando il sellaio Antonio Carra pugnalò a morte il Duca Carlo III° di Borbone.[9]

L'altro collega, Leonida Canali, fece pratica nello studio di Agostino Berenini, e già nel '22 era segnalato come soggetto pericoloso. Di tempra tenace e resistente a qualsiasi compromesso, tale atteggiamento gli costò la carriera professionale. Trovò impiego presso l'Inps a Milano, e dal settembre '43, già comunista, iniziò la sua instancabile attività politica. Denunciato il 13 Luglio '44 da un ufficiale repubblichino, arrestato, fu poi deportato a Bolzano quindi al campo della morte di Flossemburg (Baviera) dove il 16 novembre dello stesso anno fu massacrato a colpi di scudiscio e cremato, come attestano i compagni redivivi.
L'avvocato Giuseppe Barbieri, dirigente della resistenza parmense, si formò professionalmente nello studio Venturini. Venne fucilato in Piazza Garibaldi insieme ad altri 6 partigiani e antifascisti dalla brigata nera nella notte tra il 31 agosto e 01 settembre '44 sotto lo sguardo del capo del fascismo parmense, Pino Romualdi, personaggio che, come si vedrà oltre, ebbe a scontrarsi violentemente con gli avvocati parmensi.

Sopravvissero alle deportazioni colleghi come Giorgio Pavarani, che molti di noi hanno conosciuto. Tenente di vascello, fu fatto prigioniero a Patrasso all'indomani dell'armistizio e deportato a Wietzendorf. Nel campo di concentramento si dedicò alla ricerca di altri parmigiani internati, tra i quali frequentò Giovanni Guareschi e per sopravvivere teneva un diario quasi quotidiano e si impegnò nella non semplice opera della compilazione di un elenco di tutti i militari parmigiani presenti in quel momento nel campo di Wietzendorf, coadiuvato, nel primo dopoguerra, dallo studente Pietro Micheli (sarà deputato DC). Il 3 dicembre del '43 scrive alla madre dallo Stalag 328 di Leopoli, oggi in Ucraina "continuiamo a pregare e a confidare nell'aiuto divino" ove affida a Dio la moglie incinta e la salute del nascituro, raccomandando alla madre di curarla e assisterla "come farei io", affinché "il piccolo sia la sua unica preoccupazione".[10] (scrivevo queste note quando all'improvviso veniva a mancare il figlio Stefano, collega preparato, serio e schivo la cui figlia Cristina è ora avvocato e Giudice onorario penale a Parma).
Nel suo diario è scritto testualmente che si salvò da morte sicura per fame mangiando un topo morto, dividendolo con un compagno di prigionia.

Fra loro anche l'Avv. Giuseppe Bertora, padre e avo dei noti nostri colleghi. Ricorderete che, come ho scritto nella prima puntata, egli era stato direttore del giornale scolastico "Primavera" uscito nel 1922. Di lui scrisse l'Avv. Mario Ghidini, suo compagno durante la prigionia, futuro presidente provinciale della Associazione reduci di guerra (Ghidini partecipò alla campagna di Russia, poi internato in campo di concentramento, fu decorato al v.m.) "*Il capitano Bertora Giuseppe si è distinto per costante incitamento ai colleghi prigionieri alla intransigenza e resistenza alle suddette pressioni tedesche e fasciste*" Racconta ancora Ghidini "*fu catturato dai tedeschi in dipendenza degli eventi dell'08 Settembre '43 dopo aver combattuto contro gli stessi, e deportato in Germania come prigioniero di guerra" (...) dalla cattura alla liberazione ha sempre rifiutato ogni adesione sia al combattimento sia al fronte del lavoro, nonostante le sollecitazioni e le pressioni dei tedeschi e degli agenti della pseudo-repubblica, non prestando perciò mai con gli stessi collaborazione alcuna e rimanendo sempre nei lager della prigionia germanica*". Ho un ricordo lontano dell'avv. Salvatore Lauria, che svolse attività sovversive e di sabotaggio all'interno dell'esercito nonostante, come molti giovanissimi, avesse dato il suo consenso al PNF durante il ventennio.[11]

Sfuggiti alle deportazioni e più esposti degli altri, i colleghi ebrei: il già ricordato Aristide Foà nel 1943 e i due fratelli Ettore e Giacomo Ottolenghi furono i primi ad abbandonare casa e studio per riparare in Svizzera clandestinamente. Giacomo Ottolenghi, futuro senatore PSI, prima di espatriare ricoprì l'incarico di responsabile delle Delegazioni per l'assistenza ai migrati, che si rifaceva alla Unione delle Comunità israelitiche italiane ed era impegnato ad assistere gli ebrei che intendevano emigrare. Rifulse l'opera del pretore Pellegrino Riccardi che, presentendo i tempi, senza destare alcun sospetto, data la sua qualità, penetrò con aria sicura nell'ufficio comunale di Fornovo Taro attiguo alla Pretura per sottrarre carte di identità, imprimere a secco il timbro del Comune e poi, a casa, con

9 Da allora ad opera di borghesi mazziniani e di popolani molte teste rotolarono tra militari e funzionari borbonici, persino di un piemontese nel 1874: era la base del futuro sindacalismo rivoluzionario che si affrancò dalla Camera del lavoro riformista.

10 Scriverà tra l'altro nel suo diario le ragioni per cui non aderì alla RSI: "*Perché non aderisco? Anzitutto perché provo un'avversione istintiva per i tedeschi, sentimento che è entrato in me insieme al latte di mia madre, influenzato dalla guerra in atto quando nacqui e dalla narrazione della vita di prigionia del mio padrino Olindo. Inoltre per un'altrettanta nutrita avversione contro il regime fascista che pur professando ideali puri e nobili e disponendo di enormi mezzi offerti dall'intera nazione, non ha realizzato che pochissimo, permettendo invece dispersioni e ruberie infinite che hanno condotto alla rovina dell'Italia, veramente tradita dalla cricca dei governanti*". Si noti l'iniziale abbaglio ideologico, comune ai più. Anche Emilio Taverna, indimenticato professore di italiano al Liceo Romagnosi di molte generazioni, come ricorda in una testimonianza del 1956 richiestagli da Don Cavalli, allora presidente dell'Istituto Storico della Resistenza di Parma, finì nel lager di Wietzendorf destinato agli "indesiderabili": "*fame, mancanza di notizie da casa, promiscuità, le atrocità degli interpreti alto atesini e "i bambini tedeschi che ci insultavano*" (!). 4.000 ufficiali italiani rifiutarono di sottoscrivere questa dichiarazione richiesta per sottrarsi a sofferenze fisiche e morali: "*Aderisco all'idea repubblicana dell'Italia repubblicana fascista e mi dichiaro volontariamente pronto a combattere con le armi nel costituendo nuovo esercito italiano del duce, senza riserve, anche sotto il comando supremo tedesco, contro il comune nemico dell'Italia repubblicana fascista del duce e del grande Reich germanico*". Anche in Giappone agli Italiani ivi residenti che non sottoscrissero l'adesione alla R.S.I. fu riservato lo stesso trattamento (Fosco Maraini, padre di Dacia, nello stupendo autobiografico "*Case, amori, universi*" Ed. Mondadori).
Taverna rinsaldò l'autentico amor di patria con "conferenze" per i compagni italiani di detenzione, insegnando loro Manzoni e Leopardi. Alcuni suoi versi nella poesia *Germania:* "*Improvviso / lacerante / l'urlo pazzo / dei guardiani. Le saette / di quei fari / crepitare / di fucili. L'urlo freddo / della morte / sul tuo cuore / prigioniero*".

11 Molte di queste notizie sono tratte dall'articolo di Marco Minardi *"Avvocati antifascisti di Parma deportati nei campi di concentramento del III° Reich"* nel volume 22 dell'Istituto Storico della resistenza e dell'età contemporanea / Parma.

l'aiuto di un incisore, falsificò le tessere con nominativi e dati anagrafici di terzi sconosciuti. Erano destinate agli amici ebrei che avessero dovuto espatriare clandestinamente. In tal modo salvò la famiglia dell'avvocato Rolando Vigevani, approdato in Svizzera dopo varie peripezie, il cui figlio Tullio, troppo piccolo per essere esposto ai rischi del passaggio del confine, restò in Italia presso il giudice Riccardi, che se ne accreditò la apparente paternità per il tempo necessario.
Collaborarono con lui in questa opera altri tra cui il Prof. Avv. Aurelio Candian (si ricorderà, protagonista del famoso processo contro Lusignani) titolare della Cattedra di Diritto Civile a Milano. Nell'Agosto '44 entra a far parte del C.L.N. di Parma con il nome di "dott. Volpi" partecipando in qualità di partigiano non armato.
A Pellegrino Riccardi, futuro presidente della Sez. Penale del Tribunale di Parma, fu consegnata il 26.12.1988 la medaglia dei Giusti, presso l'ambasciata di Israele. Schivo come era, non si riuscì a convincerlo ad andare a Gerusalemme per piantare il suo albero nel giardino dei Giusti. Quando gli chiesero perché avesse operato assumendosi tanti rischi, rispose con semplicità: "se tutti avessero fatto quel poco che ho fatto io la Shoa non ci sarebbe stata". Che è poi la traduzione con parole semplici di un forte pensiero di Edoard Burke (1729-1797): "la sola cosa necessaria affinché il male trionfi è che gli uomini non facciano nulla" [12].

Tra i colleghi rimasti in città va nominato Paolo Venturini, socialista, nel cui studio, nel 1942 si formò il primo comitato d'azione antifascista di Parma con la partecipazione degli Avv.ti Aristide Foà, Primo Savani, Arturo Scotti oltre a Ferdinando Bernini, nonché Olimpio Febbroni, Don Cavalli e Giuseppe Micheli per i popolari. A villa Braga, del celebre clinico Angelo Braga, cognato di Giacomo Ferrari, si svolse il 9 Settembre 1943 la prima riunione, ove si decise l'organizzazione della Resistenza armata nel parmense.
A Bologna tra le file antifasciste l'Avv. Francesco Berti Arnoaldi Veli, azionista, eminente partigiano, (deceduto da pochi mesi trascorse la sua vita post Liberazione tra la professione e le testimonianze di resistente in decine di scolaresche), padre di Giovanni, attuale Presidente dell'Ordine Forense Bolognese. E l'Avv. Mario Jacchia, perseguitato ebreo, del partito d'azione, che ebbe distrutto lo studio, nel '37 fu radiato dall'albo, e passò alla lotta armata. Era nel suo studio a Bologna durante una riunione del CLN quando, preavvisato dell'arrivo dei tedeschi, restò da solo per bruciare tutte le carte compromettenti. Non fece in tempo a sfuggire alla cattura e venne ucciso a Parma il 20 Agosto 1944.
Alcuni di questi ed altri legali, costretti a darsi alla macchia, ebbero come "tutori professionali" di copertura generosi colleghi, come si vedrà nei documenti riportati nel successivo capitolo.
Partigiani combattenti furono l'avvocato Druso Parisi (Mario), Ispettore Giudiziario del Comando delegazione Est Cisa, il liberale Avv. Giorgio Mazzadi, della I° Julia, e l'avv. Enzo Costa (Ferrarini). Vennero eletti comandante capo Giacomo di Crollalanza (Pablo) e commissario di guerra Primo Savani (Mauri). Successivamente avverrà l'eccidio del comando generale di base a Bosco di Corniglio che obbligò alla ricostituzione integrale del comando militare. Succedette a Pablo, Arta, il futuro Senatore sindaco di Parma Giacomo Ferrari.
Il gruppo Fiamme Verdi sarà comandato dall'Avv. Michele Cisarri, tra i partigiani anche l'avv. Vincenzo Bianchi per "giustizia e libertà" e uomini di legge come il futuro notaio dott. Sergio Bertogalli (Mario) di parte popolare, Commissario della Brigata Pablo e suo cugino, avv. Bertogalli, al cui nome si è sovrapposto il soprannome *"Gallinò",* nativo della località Bertogallo (guarda la fantasia!). E il "dottore di legge", il partigiano Licinio Soliani.
L'avv. Enzo Costa (sarà maestro e suocero del nostro redattore capo), il futuro procuratore della Repubblica Giovanni Ardenti Morini e il funzionario delle poste dott. Domenico Tommasicchio vennero tutti e tre arrestati per una spiata. Intervennero a favore di Ardenti Morini il procuratore del Re dott. Contino, padre del ben noto Avv. Giuseppe Contino e il vescovo di Parma, ma Tommasicchio fu barbaramente ucciso[13].
Ancorché al di fuori della cerchia forense ricordo anche due futuri validissimi e apprezzati dentisti, il Dott. Ottavio Braga detto Dodo (Rolando) Commissario della 32esima Brigata Garibaldi "Monte Penna" e il Dott. Bruno Casa (capo servizio sanitario del Comando delegazione Est Cisa). Quest'ultimo fu partigiano insieme a quella che sarà sua moglie, Argia Tedeschi, staffetta che meritò la medaglia di bronzo. Il dott. Casa e il Dott. Brunetto Ferrari, figlio del comandante Arta, operarono insieme un ferito, ma per Brunetto doveva essere la prima ed ultima sua operazione chirurgica[14]. Il suo nome fu tramandato a figli dei partigiani, come il figlio dello stesso dott. Casa, genitore a sua volta del giovane collega Casa Carattini.
E ancora il noto artista parmigiano Ubaldo Bertoli (Gino), prestigioso pittore con forte carica satirica e autore de la "Quarantasettesima", ben noto racconto partigiano, Ed. Einaudi.
La quarantasettesima brigata Garibaldi, era definita "delle teste calde" dal maggiore inglese Charles Holland

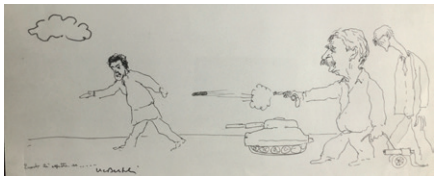
12 Dal racconto del nipote Carlo Bocchialini: *"Riccardo Pellegrini un giusto tra le Nazioni"* (Guaraldi-Lab Atelier 65 Editore)

13 L'avv. Enzo Costa è stato esempio di virtù e dignità militare. Venne delegato da Savani (che sarà il primo sindaco di Parma eletto) a trattare con i tedeschi lo scambio di prigionieri. Si puntava in particolare sulla liberazione di un tenente tedesco, a cui i nazisti tenevano molto, fatto prigioniero nel piacentino. La scelta cadde sull'avvocato Costa dato che operava nel comando nord emilia in qualità di commissario politico: libertà a Costa per operare, Savani si sarebbe costituito ai tedeschi se entro il 31.12.1944 non fosse tornato a missione compiuta. Identico trattamento per l'avvocato Costa, si offrì volontariamente anche Paolo il danese, figura leggendaria, prima monaco benedettino in Danimarca, poi ordinato sacerdote cattolico a Roma, infine partigiano "bianco" nelle montagne del parmense, con intermezzi vari tra cui quello di precettore dei Meli Lupi di Soragna nella loro villa a Vigatto. Costretto ad uccidere un nemico, ritenne ciò incompatibile con il sacerdozio, a cui rinunciò. Sposò una partigiana ed ebbe tre figli, di cui uno vive nella nostra provincia. Decorato con medaglia d'argento al v.m.. Una storia affascinante, ma anche misteriosa (probabilmente era dell'intelligence inglese). Direi un Garibaldi cristiano. Particolarmente documentata la biografia di Thomas Harder "Paolo il danese - un prete partigiano" – Ed. Mattioli 1885. Ma torniamo allo scambio di prigionieri. Si verifica un incidente: il tenente tedesco che doveva essere liberato venne ucciso dai partigiani in un tentativo di evasione. Costa e Savani (entrambi comunisti) ebbero il coraggio di ripresentarsi al comando tedesco per riferire l'accaduto. I partigiani avevano già liberato 88 prigionieri tedeschi, loro 165 tra partigiani e familiari. Dopo un primo momento agghiacciante, all'avv. Costa i tedeschi impartirono l'ordine di restituire le spoglie del loro tenente, termine tre giorni. Costa avrebbe potuto non ottemperare, nascosto come era tra i monti, ma a prezzo di possibili ritorsioni riportò a Fiorenzuola la salma. Fu decorato con medaglia d'argento al v.m.

14 "In una casupola, mentre d'intorno si sparava, fecero bollire una sega da falegname, prima da una parte e poi dall'altra, in una pentola d'acqua. Il paziente era tenuto fermo da altri partigiani. I due chirurghi improvvisati, sotto gli occhi esterrefatti dei presenti e del paziente, che non emise un gemito di dolore, uno da una parte e l'altro dall'altra parte della sega, asportarono il troncone orami tumefatto del braccio colpito. Compiuta l'operazione, una fasciatura, come era possibile in quelle condizioni. Vittorio guarì. Rimase nelle formazioni partigiane fino alla fine della guerra ed ebbe il comando di un battaglione". (...) "Ormai anche noi avevamo il nostro Maroncelli". (Primo Savani *"Antifascismo e guerra di liberazione a Parma"*, pag. 133, Guanda Ed.).

[15], paracadutato dietro le linee tedesche; e Leonardo Tarantini già tenente dell'esercito (Nardo), comandante della divisione garibaldina Ottavio Ricci, di sperimentate doti militari, sarà a lungo presidente dell'ANPI locale.
E poi l'ardimentoso partigiano Avv. Lanfranco Fava, Enzo Baldassi, futuro sindaco della città. Nato nei monti e combattente tra i monti il "partigiano bianco" Guglielmo Cacchioli (Beretta) comandante della divisione "Cisa".
Si unirono a loro successivamente i più giovani come gli studenti Aldo Cremonini, allora liberale, militante nella terza brigata autonoma "Julia" comandata da Paolo il Danese (Arndt Paul Richardt Lauritzen); e Aminta Rota, noto come "comandate Gallo", futuro notaio. [16]

15 Cifra di questa definizione lo stesso disegno – autoritratto di Bertoli partigiano, qui accanto, che spara con una pistola "a spruzzo": alle sue spalle il pittore Carlo Mattioli.
In fondo a sinistra si legge: "Questo ti aspetta se ..."



16 Mi piace ricordare anche il Prof. Italo Podestà, partigiano cristiano, antifascista della prima ora, proveniente da Pontremoli. Fu professore al Romagnosi prima di diventare preside dell'Istituto magistrale. Incedeva a testa alta, i pensieri avvolti in Kierkegard e nei testi di Sant'Agostino, che poi distillerà in poesie intimistiche e cristianamente ispirate. Sia concesso in un testo serioso la citazione di un folgorante "schizzo" che fecero di lui gli studenti in una finta intervista in un giornale scolastico. "Alla richiesta rivolta ad alcuni professori di un giudizio su Sophia Loren il prof. Podestà ha risposto: "*Bisogna vedere se può essere pensata. Può darsi che non sia oggetto di pensiero*".

Un posto a parte va dedicato a Giacomo Ulivi, studente liberale proveniente dal convitto Maria Luigia. Venne fucilato a Modena in Piazza Grande nel novembre 1944 per le sue ardimentose imprese antifasciste. Fu decorato della medaglia d'argento al valor militare alla memoria. L'ultima lettera agli amici, quasi un testamento spirituale: "*Credetemi, la "cosa pubblica" è noi stessi; ciò che ci lega ad essa non è un luogo comune, una parola grossa e vuota, come "patriottismo", o amore per la madre che in lagrime e in catene ci chiama, visioni barocche, anche se lievito meraviglioso di altre generazioni. Non siamo falsi con noi stessi, ma non dimentichiamo noi stessi, in una leggerezza tremenda. Al di là di ogni retorica, constatiamo come la cosa pubblica sia noi stessi, la nostra famiglia, il nostro lavoro, il nostro mondo, insomma, che ogni sua Sciagura è sciagura nostra, come ora soffriamo per l'estrema miseria in cui il nostro paese è caduto: se lo avessimo sempre tenuto presente, come sarebbe successo questo?".*
Divenne amico del suo Prof. Attilio Bertolucci a cui aveva scritto dal carcere pochi giorni prima di morire, una lettera recapitata dalla madre.
Il suo prof. di latino e greco, Italo Petrolini, scrisse di lui: "*Con gli occhi acuti, mai fermi, cui nulla sfuggiva del professore e dei compagni, seduto come se fosse pronto a scattare ad agire, e gentile, sereno, entrava con un largo sorriso di saluto, contento ogni giorno di apprendere, di confrontare idee, di superare difficoltà. Il compito in classe in latino e greco direi che per lui era una festa dello spirito: era così veloce nel finire la traduzione molto prima delle due ore di tempo concesse, che, anche per tenerlo a bada (però con che discrezione sapeva soccorrere compagni in difficoltà) tenevo pronto un secondo tema per lui, più denso e impegnativo del primo".*[17]
Con lui ricordiamo altri giovani, come Giordano Cavestro, studente comunista, fucilato dai nazisti a 19 anni, medaglia d'oro al valor militare alla memoria, che scrisse una oramai celebre lettera inserita tra quelle dei condannati a morte della Resistenza. E Marco Pontirol Battisti, studente liceale al Romagnosi, morto in combattimento a soli 17 anni, insignito della medaglia d'argento al valor militare alla memoria.

Raccontavano i nostri colleghi partigiani delle notti illuminate dalla luna piena sui monti, in attesa dei paracaduti degli alleati. I più erano bianchi, destinati alle armi e alle vettovaglie, ma taluno, nella nostra zona, rossi: erano quelli contenenti il danaro. La loro distribuzione avveniva su disposizione del comandante Mauri cioè l'avv. Primo Savani. Nelle lunghe attese dei lanci esprimevano i loro desideri: cosa vorresti quando tutto, finita la guerra, sarà tornato alla normalità? Io –diceva il comandante Maurimulinando il braccio come era nella sua gestualità, vorrei fare un buco grande grande in quella montagna e ci farei passare una strada per congiungere Parma al mare. E così quando divenne Presidente della Provincia fu costruita

17 Giacomo Ulivi fu simbolo della borghesia liberale e democratica (due aggettivi che di questi tempi stentano a coesistere) di impronta gobettiana - componente importante della Resistenza a Parma. Nella foto accanto una bella immagine della madre di Giacomo, Maria Luisa Fornari, abbracciata ad Aldo Cremonini.
Al di là di quanto da sinistra (... Dante Gorreri) sottovoce e con malizia si diceva, essere il contributo alla Resistenza di certi intellettuali "da salotto" (rimando alla seconda puntata di questo mio scritto) limitato alla esterofilia (della cultura o ... dell'abbigliamento inglese), nella borghesia cittadina saranno i liberali ad animare la stagione post bellica politica e culturale pubblicando *"l'uomo libero "*diretto da Baldassarre Molossi. Vi scrivevano gli avvocati Cremonini e il giovanissimo Fabio Fabbri. Poi, con il "malagodismo", la diaspora dei radicali, che strappò il tessuto della borghesia. Furono polemiche accese. Usciva un grande manifesto dei liberali: "l'uomo libero è liberale". Replicavano i radicali: una verza enorme con scritto "L'uomo vegeto è vegetale", e poi andando oltre il periodo esaminato, quell'originale partito radicale di Parma composto da tutti uomini di legge, da contarsi sulle dita delle mani: gli avv.ti Cremonini, Contino, Olivieri, Fabbri, Avanzini e il notaio Aminta Rota, e da ultimo l'Avv. Ponzone. Mentre la vita del Paese, che versava nei momenti più acuti della guerra fredda, era connotata da scioperi spesso cruenti (Reggio Emilia, Genova) e dalla lotta di classe.
Se in tutta Italia dominava la cultura marxista o comunque di sinistra, a Parma nel 1953 Attilio Bertolucci, Pietrino Bianchi, Luigi Malerba e Virginio Marchi, con il sostegno dell'industriale Pietro Barilla, celebrarono il primo e storico convegno sul neorealismo, a pluralistico dialogo culturale.

la Parma – Mare.
Il più giovane Aldo Cremonini, padre del nostro collega Carlandrea, dopo i lanci ritagliava le sete dei paracaduti per donarle alle ragazze per il loro abbigliamento.

In questo tragico arco temporale, tra bombardamenti, rifugi, rastrellamenti e divisioni laceranti all'interno delle famiglie, tra gli amici e tra i nostri colleghi, vi fu una solidarietà anche trasversale e clandestina sui due opposti fronti. Ben 12 anni fa, su queste colonne, ho raccontato un episodio, che ripeto per i più giovani.
Nello stesso studio in Parma erano due avvocati, uno l'avv. Vittorino Ortalli, federale della città, l'altro l'Avv. Druso Parisi, appartenente al locale C.L.N. e comunista. Che l'uno sapesse dell'altro era evidente, ma anche che Ortalli si avvedesse e fingesse di non vedere le riunioni clandestine degli antifascisti. Un saluto, un sorrisino e via. Ortalli, di origine fidentina, iscritto al PNF prima del compimento dei suoi 14 anni, era un professionista e persona per bene, non aveva torto un capello a nessuno, uomo arguto e brillante penalista (e tuttavia gravitava nell'orbita di Farinacci[18]).
Ci si misero di mezzo però le camice nere che tenevano d'occhio Parisi. La soffiata: Paola, l'impiegata comune dello studio, viene a sapere che i fascisti verranno per perquisire lo studio di Parisi e portare via tutto, mobili e pratiche, per impedirgli di lavorare. Che ti fa lei, staffetta partigiana? In una sola notte trasferisce lo studio di Parisi in quello di Ortalli e viceversa. Sicché quando le camice nere arrivano e chiedono dove si trovi lo studio di Parisi, l'impiegata indicava quello "reale", prima del trasloco notturno. E così mobilio, pratiche e suppellettili appartenenti al federale vennero messi sotto sequestro in Prefettura. Nonostante la grande amicizia tra i due, l'irritazione, a dir poco, dell'imbarazzato Federale. Ma poteva andar peggio: perché lui non lo sapeva, ma sotto il pavimento della vera stanza di Parisi c'era un deposito di armi. Quando Vittorino fu festeggiato nel cinquantennio con la toga d'oro non mancò di ricordare e di far mettere a verbale che, nonostante le opposte posizioni politiche, l'amicizia con Druso restò forte e incrollabile tranne "per quella *stronzata dei mobili"* (testuale).
La vita riserverà altre curiosità. Dopo la liberazione Ortalli fu ristretto nel carcere di Cremona, della cui città era podestà. L'allora Guardasigilli Togliatti nominò P.M. della Corte d'Assise straordinaria di Parma gli Avv.ti Primo Savani e Druso Parisi[19]. Gli è che costoro andavano continuamente a Cremona per interrogarlo. Ma come, non lo conoscevano come le loro tasche? Si seppe poi che in realtà fungevano … da taxi per la moglie e il figlio perché potessero incontrarsi.
Dai famigliari dei colleghi partigiani, che non ci sono più, ho appreso che queste carcerazioni di ex fascisti erano volute dal Ministro della Giustizia Togliatti, lo stratega della svolta di Salerno, per sottrarli alle vendette che si consumavano per lo più nel vicino "Triangolo della morte". A sua volta Parisi, quando veniva a sapere che qualche fascista era in pericolo, subito lo faceva chiudere nel carcere minorile Lambruschini, alla Certosa, per impedire ulteriori eccidi. Nello stesso senso operò Paolo il Danese, nominato direttore delle carceri di Parma. Intervenne l'amnistia. Allora qualche ex partigiano veniva a trovarsi a stretto contatto tra i tavolini dei caffè di Piazza Garibaldi con i fascisti che aveva appena condannato a morte. Un sobbalzo degli uomini di legge di ceto liberale che in quella condanna erano stati coinvolti, messi in minoranza o psicologicamente aggregati dagli uomini più di sinistra. Certo, momenti di passaggio a cui seguiranno gli ulteriori, inevitabili sviluppi e differenziazioni.
Ma ci furono anche momenti di *stress* e di malcelata ilarità, a cui non si sottrasse la celebrazione di processi ordinari – non politici – come quello che esplose nella attuale Aula Mossini del Tribunale, in pieno periodo bellico, quando si "andava a sentenza" previa discussione orale. Un giorno, in udienza collegiale, un avvocato comincia a parlare, a straparlare, a gridare frasi senza senso. Tutti si appartano, sconcertati. Resta un avvocato del regime, cultore di diritto corporativo, che con il suo vocione virile intima al folle di smetterla e di darsi una disciplina. Ma quello ha uno scatto: "taci tu che sei l'avvocato più stupido di tutta Parma". Nascosto dietro il banco riservato ai giudici, l'avv. Gamaliele Ghidini, fratello del Prof. Mario, e figlio dell'Avv. Gustavo, fa capolino e con voce spaurita commenta: "Attimo di lucido intervallo". E si ritrae. Niente da fare. Dovette essere condotto in autoambulanza nel vicino paese padano, a *quattro pazzi* dalla Reggia Ducale. Altra vittima bellica.[20]
Seguono i documenti a cui ho più volte accennato.

La fermezza del sindacato forense di Parma

Il 31 maggio 1944 il commissario della Federazione fascista repubblicana di Parma Pino Romualdi inviò al sindacato forense ed al capo della provincia di Parma la seguente lettera: "*Risulta che per quanto alla macchia, gli avvocati Parisi Druso, Savani Primo, Venturini Paolo, Fava Lanfranco, regolarmente denunciati al Tribunale straordinario provinciale, continuano a far funzionare i loro uffici tramite l'interessamento di altri colleghi che li sostituiscono. Il sostituto dell'avv. Parisi risulta l'Avv. Belli Antonio, quello di Savani Candian, quello di Venturini Bordi e quello di Fava l'Avv. Calzolari* (Giovanni, Guido era deportato, ndr).
1) Gli avvocati Parisi, Savani, Venturini e Fava siano radiati dall'albo professionale;
2) Siano chiusi gli uffici legali di codesti avvocati e le pratiche tuttora inevase siano affidate al Sindacato avvocati per la ripartizione tra professionisti di buona moralità professionale e politica.
Chiedo inoltre che le autorità di pubblica sicurezza accertino quale sia il grado

18 Con quel certo riguardo, oggi in uso nel linciaggio politico, il 03.08.1938 Farinacci scriveva a Mussolini: "*Caro Presidente, è vero che la madre del Papa è una ebrea? Se fosse vero sarebbe un vero spasso. Parto questa sera per Cremona dove mi basterebbe un semplice cenno*"

19 Già prima gli alleati furono meravigliati, appena giunti a Parma, di trovare la città in perfetto ordine e con tutti i servizi funzionanti. "*I loro Tribunali erano nelle colline intorno alla città e, a quanto dicono i funzionari del Governo militare alleato, sotto i partigiani la legge e l'ordine pubblico funzionavano a meraviglia*" (Radio Londra 28.04.1945 da "Antologia della Resistenza" di Luisa Sturari).

20 Merita una noticina a parte un nostro collega, federale di Parma nel 1925. Bizzoso e stravagante, alternò momenti di fideismo e di critica interna, tanto da essere più volte espulso e poi riammesso nel P.N.F. Diventò sempre più critico dopo aver combattuto in Libia sino a manifestarsi ostile al regime verso la fine del 1941. Eppure nel suo studio aveva alle spalle un enorme ritratto del ras di Cremona perché tutti capissero che aveva la approvazione di "Roberto", cioè di Farinacci, e di "Alfredo", cioè il ministro Rocco. Come già ho ricordato tempo fa, aveva sulla scrivania due telefoni, uno reale, l'altro fasullo, che faceva squillare a comando per rispondere sbuffando per il continuo disturbo, a immaginarie chiamate del Duce e di alti gerarchi: con grande stupefazione dei clienti. Nell'aprile del '44 assunse la difesa di partigiani del distaccamento Griffith davanti al Tribunale militare; così come dopo il 25 aprile difese imputati fascisti davanti alla Corte d'Assisi straordinaria. Nel febbraio '45 era divenuto lui stesso partigiano nella brigata II° Julia di tendenza democristiana. Fece però un passo azzardato. Alla festa della liberazione si presentò a Berceto tra i partigiani in sella ad un cavallo bianco "anche se un po' spelacchiato". Ma alcuni partigiani lo riconobbero, ed il nostro avvocato nonché commendatore dovette scendere da cavallo e dileguarsi sui monti per alcuni giorni. Il Giuffredi e il Savani nelle opp. citt. convergono nel racconto. Però, mentre il primo nomina espressamente il collega, Savani si limita ad ammiccare. Io obbedisco al Comandante Mauri.

di complicità dei nominati avvocati Belli, Candian, Bordi e Calzolari coi colleghi latitanti e se mai abbiano presentato a cause ultimate documenti e quietanze da questi ultimi regolarmente firmate. Se ciò risulterà vero gli stessi dovranno essere denunciati per il reato di complicità e immediatamente radiati dall'Albo.

F.to Pino Romualdi".

Ed ecco la risposta del presidente del Sindacato forense:
"7 giugno 1944. Al Capo della Provincia di Parma.
In relazione a quanto comunicatomi verbalmente in ordine al foglio Ris. 77 del 31 maggio u.s. della Federazione fascista repubblicana, Vi rendo noto che interpellato il Direttorio del Sindacato ed esaminata la legge professionale, si è ritenuto non essere possibile la radiazione degli avvocati Parisi, Savani, Venturini e Fava, in quanto il provvedimento della radiazione non può essere emanato se non quando sia stata inflitta condanna penale, non potendo il giudizio disciplinare precorrere, e ciò allo scopo di evitare conflitto di giudicati.
Inoltre non può essere disposta la radiazione o la sospensione di cui agli artt. 42-43 della legge stessa 22 gennaio 1934 n. 36: in quanto la prima è condizionata alla condanna a pena non inferiore nel minimo ai due anni, e la seconda alla emissione e comunicazione del mandato di cattura da parte delle autorità competenti.
Per quanto riguarda l'attività svolta dai colleghi che hanno sostituito nelle cause in corso i professionisti suddetti, si accerta che nessuno istanza di liquidazione, quietanza od altro documento a firma dei detti professionisti è stata presentata a questo Sindacato.

F.to Avv. P. Boselli"[21]

Il crepuscolo

Era una domenica di primavera, una giornata tiepida e dal cielo terso e azzurro, irripetibile, da godere tutta prima che la calura divampasse dalla terra e nell'aria. Poteva essere l'anno 1969 o '70, quando si era appena celebrato il 12esimo congresso del P.C.I. Con Gianni Ferrari e rispettive mogli si decide di andare sull'Appennino, senza meta fissa, forse all'inconsapevole ricerca di incontri. A Bosco di Corniglio una sosta presso il ben noto albergo Ghirardini, di fianco a quello che era stato il Comando unico Partigiano.
Qui sopravviene l'Ing. Giacomo Ferrari, che fu Sindaco di Parma, Ministro dei Trasporti e Senatore della Repubblica, prima ancora prefetto di Parma dopo la Liberazione. Figura preminente del comunismo parmense, era zio di Gianni, il quale però professava un credo politico di impronta socialista e riformista. Come si è già accennato, Giacomo Ferrari aveva un'ascendenza familiare mazziniana, che pochi conoscevano. Racconta dal vivo l'eccidio di Bosco di Corniglio. Metà Ottobre '44.
Il traditore Mario lo slavo, il carbonaio che dall'alto, fucile dei nazisti piantato nella schiena, doveva far loro strada per condurli al Comando unico, e lui che traccheggiava, sceglieva i sentieri più lunghi per fare in modo che i tedeschi arrivassero il più tardi possibile, quando i partigiani fossero svegli, e loro ad intimargli di far presto, avevano capito il gioco. Arrivarono alle 5 del mattino e piazzarono una mitragliatrice "proprio lì" e cominciarono a sparare a raggiera da sinistra a destra, e viceversa, tra una casa e il comando, proprio verso la valle. Alcuni, tra i quali Parisi, si salvarono gettandosi dalla finestra al primo piano proprio quando il mitra sparava sul lato opposto, rotolando nel burrone vicino.
Molti i morti, tra questi il comandante Giacomo di Crollalanza (Pablo): ufficiale di carriera, 27 anni, gli furono conferite la medaglia d'oro al v.m. e la laurea ad honorem in ingegneria.
Nella notte tornarono i sopravvissuti uno alla volta, circospetti: contarono i caduti, li composero e li vegliarono. Con loro era accorso Parisi, che sarà P.M nel processo che si concluse con la condanna a morte del traditore[22]. Il comando, dopo una riunione in chiesa, dovette essere interamente ricostituito e fu nominato comandante unico, successore di Pablo, lui, Arta. Il quale, dopo il racconto, ebbe un'idea: andiamo a Casarola a trovare Attilio Bertolucci. Abitava in una modesta villetta con la moglie Evelina Giovanardi, Ninetta, la fanciulla bionda che aveva conosciuto tra i banchi di scuola. ("*Penso a una fanciulla bionda. – Fra poco sarà mezzogiorno – e una gran tenerezza m'invade, - e una voglia di piangere senza perché".)*
Erano in ansia, in attesa di notizie dei figli Bernardo e Giuseppe che si trovavano molto lontano, all'estero. Da pochi anni era uscito sugli schermi, girato a Parma, "Prima della rivoluzione" di Bernardo, oggi considerato come una anticipazione della contestazione del '68.
Gli incontri significativi non finirono lì perché all'uscita c'erano alcuni manovali che eseguivano lavori di restauro alla villa. Uno di loro si illumina: Senatore non mi riconosci, la mozione di minoranza al congresso Provinciale PCI (quella filosovietica all'indomani della invasione della Cecoslovacchia ndr), l'abbiamo votata solo in due: l'altro ero io !
Era davvero il crepuscolo della giornata, ma anche delle ideologie, tuttavia nessuno lo percepì. Solo più tardi, leggendo "L'insostenibile leggerezza dell'essere" di Milan Kundera compresi che i tempi erano maturi. Il ghiaccio si sciolse e divenne liquido. Poi cominciò a formarsi la caligine. E non si vede più come prima.

Profili storici dell'Avvocatura

Conseguenza della loro formazione, il ruolo essenziale degli avvocati nel consolidamento *iniziale* dell'Unità d'Italia, inteso come collegamento tra il cittadino e gli enti pubblici territoriali, Parlamento e Governo (v. tra noi l'Onorevole Agostino Berenini già sindaco della città, fu protagonista di celebri processi come quello del caso Murri), salvo note negative quale il sistema tendenzialmente clientelare e vicino alle formazioni lobbystiche.[23]
La trasformazione da umanisti "prestati" alla scienza giuridica e alla pratica forense a imprenditori (libera concorrenza, abolizione dei minimi tariffari, pubblicità informativa) secondo una linea di tendenza derivata da direttive del Parlamento europeo e da sentenze della Corte di Giustizia, tuttavia non

21 La rilevanza della superiore risposta è rimarcata dal fatto che era stata data dal Sindacato Forense Fascista. Come noto gli ordini vennero gradualmente soppressi dal 1926 al 1933 per essere sostituiti dai sindacati forensi, nel tentativo di ricondurli al sistema corporativo. E tuttavia restarono differenziazioni: ad es. nella vicenda relativa agli esami di accesso alle istanze "riduttive" dell'avvocatura contrastarono più di una volta le spinte politiche di regime ad allargare il reclutamento e a privilegiare l'accesso dei giovani, meglio se muniti di requisiti fascisti. Quanto invece alla "questione ebraica" i sindacati applicarono il d.l. del 1938 che ordinava la cancellazione dall'albo degli avvocati ebrei, il cui ricorso per assenza di contraddittorio fu respinto dal Consiglio Forense intendendosi legge imperativa da applicarsi automaticamente. Nell'immediato dopoguerra, ricostituiti gli ordini degli avvocati, gli ebrei furono reintegrati d'ufficio, epurati (provvisoriamente) i gerarchi fascisti (cfr. Antonella Meniconi "La maschia avvocatura" – Istituzioni e professione forense in epoca fascista) 1922 – 1943 Ed. Il Mulino a cura del C.N.F.)

22 Nel novembre del '44 il cappellano della 31° brigata Garibaldi Don Nino Rolleri, che ho personalmente conosciuto e apprezzato per saggezza ed equilibrio, celebrò una messa in onore dei caduti di Bosco di Corniglio sul sagrato della chiesa di Pellegrino Parmense alla presenza delle Brigate della Val Ceno.

23 Maria Malatesta "Professionisti e gentiluomini" Einaudi 2006, Antonella Meniconi "La maschia avvocatura", Ed. Mulino 2006, a cura del C.N.F.; Gramsci "Quaderni dal carcere". "Intellettuali ed organizzazione della cultura" Einaudi 1952, pag. 11; nonché richiamo il mio scritto su Cronache dal Foro Parmense 2007 n. 1 pag. 57

adeguatamente adattate alle esigenze del nostro Paese, come sarebbe stato possibile e legittimo; da generici come medici condotti a specializzati: indirizzo che il regime deviò creando uffici legali interni ad Enti e sindacati accentrati, trattandoli come semimpiegati, con nocumento della libera professione.
Oggi invece si assiste ad una trasformazione in senso privatistico: in luogo del rapporto fiduciario con il cliente si ha l'inserimento dei professionisti nelle decisioni manageriali e nei meccanismi delle imprese o delle associazioni, con il rischio del venir meno della indipendenza professionale; in luogo del legale – artigiano l'associazione professionale interdisciplinare; il mai risolto ed anzi aggravato problema del sovraffollamento degli albi già denunciato da Piero Calamandrei nel lontano 1921 nella sua opera "Troppi avvocati!", e declino economico della professione; il superamento della questione di genere (nel 1937, a Parma, Adelina Giandebiaggi proveniente dal Liceo Romagnosi, prima iscritta all'Ordine degli Avvocati), in virtù della legge n. 1776 del 1919 -dopo il noto caso negativo di Lidia Poet- Cass. 1884 – legge osteggiata nel periodo fascista in nome dei valori della famiglia, della campagna demografica e della misoginia (un deputato arrivò a definire la legge del '19 "frenesia erotica"); solo con la legge 66 del 09.02.1963 fu consentito l'accesso delle donne a tutte le cariche, professioni ed impieghi pubblici, magistratura inclusa (la prima a Parma la dottoressa Grazia Rota): oggi le donne stanno per diventare maggioranza nell'ambito giudiziario; la spinta propulsiva della carta costituzionale come *domina* della legge ordinaria e della interpretazione giurisprudenziale, e aperta a nuovi diritti.

Giacomo Voltattorni

FINE

(nel prossimo numero stralci del diario di Piero Calamandrei combattente durante la prima guerra mondiale, di cui è appena ricorso il centenario)

Giurisprudenza Disciplinare

CORTE SUPREMA DI CASSAZIONE

la suitas, quale elemento soggettivo (sufficiente) dell'illecito disciplinare

Al fine di integrare l'illecito disciplinare sotto il profilo soggettivo è sufficiente l'elemento psicologico della suità della condotta inteso come volontà consapevole dell'atto che si compie, giacché ai fini dell'imputabilità dell'infrazione disciplinare non è necessaria la consapevolezza dell'illegittimità dell'azione, dolo generico e specifico, essendo sufficiente la volontarietà con la quale l'atto deontologicamente scorretto è stato compiuto (*Nel caso di specie, in applicazione del principio di cui in massima, la Corte ha respinto il ricorso proposto avverso Consiglio Nazionale Forense - pres. f.f. e rel. Picchioni - sentenza n. 255 del 28 dicembre 2017*).

Corte di Cassazione (pres. Mammone, rel. Armano), SS.UU, sentenza n. 30868 del 29 novembre 2018

richiesta dolosa di pagamenti già adempiuti

Costituisce gravissima violazione dei doveri di probità, dignità e decoro (art. 9 ncdf, già art. 5 codice previgente), tale da rendere incompatibile la permanenza dell'iscritto nell'albo forense, il comportamento dell'avvocato che -in esecuzione di un medesimo disegno criminoso- promuova numerose azioni esecutive su titoli già adempiuti, approfittando della fiducia (malriposta) del debitore, così indotto a pagare somme non dovute per diversi milioni di euro (*Nel caso di specie, il professionista aveva richiesto il pagamento di numerosi debiti già soddisfatti, adducendo a propria asserita discolpa il fatto che debitore avrebbe dovuto accorgersene e quindi rifiutare la richiesta truffaldina. In applicazione del principio di cui in massima, la Corte ha respinto il ricorso proposto avverso Consiglio Nazionale Forense - pres. f.f. e rel. Picchioni - sentenza n. 255 del 28 dicembre 2017, che aveva ritenuto congrua la sanzione disciplinare della radiazione*).

Corte di Cassazione (pres. Mammone, rel. Armano), SS.UU, sentenza n. 30868 del 29 novembre 2018

doveri del difensore che abbia rinunciato al mandato

E' solo la cancellazione dall'albo a determinare la decadenza del professionista dall'ufficio di procuratore ed avvocato e a far quindi cessare lo *jus postulandi*, il cui venir meno comporta altresì la perdita da parte del difensore della legittimazione a compiere e ricevere atti processuali per conto del cliente. In mancanza della stessa, non può assumere alcun rilievo la cessazione di fatto dell'attività professionale, la quale, anche quando si traduce nella rinunzia al mandato, non dispensa il difensore dal compito di ricevere la notificazione degli atti e darne notizia al cliente, in adempimento del dovere di diligenza professionale a lui incombente, a meno che non si sia provveduto alla sua sostituzione con un altro avvocato e la stessa sia stata ritualmente portata a conoscenza delle controparti e dell'ufficio.

Corte di Cassazione (pres. Manna, rel. Mercolino), SS.UU, sentenza n. 487 del 10 gennaio 2019

poteri giurisdizionali del C.N.F.

La mancata costituzione di un'apposita sezione disciplinare all'interno del Consiglio nazionale forense ex art. 61, comma 1, L. n. 247/2012 non incide sulla natura giurisdizionale dei suoi poteri, né sull'imparzialità e sull'autonomia dell'organo giudicante, le quali sono comunque assicurate dalla sua composizione collegiale e dalla natura elettiva dei suoi componenti.

La giurisdizione professionale -conosciuta anche dagli ordinamenti di altri Stati- è conforme all'art. 6, par. 1, della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (ratificata in Italia con L. 4 agosto 1955 n. 848), giacché i membri dei collegi professionali partecipano al giudizio non già come rappresentanti dell'ordine professionale, e quindi in una posizione incompatibile con l'esercizio della funzione giurisdizionale, bensì in una posizione di "terzietà", analogamente a tutte le

magistrature.

L'attuale assetto del Consiglio Nazionale Forense risulta compatibile con i principi costituzionali di terzietà ed imparzialità del giudice, atteso che la sua peculiare posizione di giudice speciale vale da sola ad escludere condizionamenti da parte di organi amministrativi in posizione sovraordinata.

Con riguardo all'indipendenza del giudice, all'imparzialità dei giudizi e alla garanzia del diritto di difesa, è manifestamente infondata, in riferimento agli artt. 24, 97 e 111 cost., la questione di legittimità costituzionale delle disposizioni sul procedimento disciplinare innanzi al Consiglio nazionale forense, a nulla rilevando in contrario la circostanza che al CNF stesso (così come, peraltro, al Consiglio di Stato e alla Corte dei Conti) spettino anche funzioni amministrative, in quanto non sarebbe la mera coesistenza delle due funzioni a menomare l'indipendenza del giudice, bensì il fatto che le funzioni amministrative fossero affidate all'organo giurisdizionale in una posizione gerarchicamente sottordinata, essendo solo in tale ipotesi immanente il rischio che il potere dell'organo superiore indirettamente si estenda anche alle funzioni giurisdizionali.

Le decisioni assunte dal Consiglio nazionale forense sono rese da un organo giurisdizionale (giudice speciale istituito dal d.lgs.lgt. 23 novembre 1944, n. 382, art. 21 e tuttora operante, in forza della previsione della VI disposizione transitoria della Costituzione), in base a norme che, quanto alla nomina dei componenti del medesimo CNF ed al procedimento di disciplina dei professionisti iscritti al relativo ordine, assicurano, per il metodo elettivo della prima e per le sufficienti garanzie difensive proprie del secondo, il corretto esercizio della funzione giurisdizionale, affidata al suddetto organo in tale materia, con riguardo all'indipendenza del giudice ed alla imparzialità dei giudizi.

Corte di Cassazione (pres. Spirito, rel. Doronzo), SS.UU, sentenza n. 2084 del 24 gennaio 2019

oneri informativi in caso di rinuncia o revoca del mandato

I doveri di informazione e di comunicazione dell'avvocato nei confronti della persona già assistita persistono sia nell'ipotesi di rinuncia che di revoca del mandato, anche se il codice deontologico della professione forense disciplina solo la prima fattispecie, atteso che la revoca del mandato costituisce, al pari della rinuncia, una soluzione di continuità nell'assistenza tecnica e, pertanto, deve ritenersi fonte dei medesimi obblighi necessari al fine di non pregiudicare la difesa dell'assistito. (*In applicazione di tale principio, la Corte ha confermato la sanzione dell'ammonimento irrogata dal C.N.F. ad un avvocato che aveva omesso di comunicare al cliente la propria rinuncia al mandato ed il rinvio di udienza, precludendogli una più opportuna difesa a mezzo di memoria istruttoria con eventuale nuovo difensore*).

Corte di Cassazione (pres. Spirito, rel. Oricchio), SS.UU, sentenza n. 2755 del 30 gennaio 2019

appropriazione indebita di somme incassate per conto del cliente

L'avvocato è tenuto a dare immediata comunicazione al proprio cliente delle somme incassate per suo conto ed a fornirgli comunque, senza necessità di particolari inviti e richieste, il rendiconto delle operazioni eseguite in applicazione della obbligazione ricadente sul mandatario, non trovando applicazione il principio della compensazione quando questo sia il frutto di unilaterale appropriazione di somme che egli abbia presso di sé per conto del cliente, quando manchi il consenso di questi (*Nel caso di specie, il professionista aveva incassato per conto del cliente ma trattenuto per sé circa 140 mila euro in buoni postali. In applicazione del principio di cui in massima, il CNF ha ritenuto congrua la sanzione della sospensione disciplinare di un anno*).

Consiglio Nazionale Forense (pres. f.f. Picchioni, rel. Salazar), sentenza del 12 settembre 2018, n. 105

appropriazione indebita di somme della procedura

L'appropriazione di somme mediante abuso della disponibilità ottenuta per ragioni di ufficio in veste di delegato dal Giudice, quindi con approfittamento della funzione pubblica, costituisce comportamento gravissimo che lede enormemente l'immagine della professione forense ed in quanto tale giustifica la massima sanzione disciplinare (*Nel caso di specie, il professionista delegato era stato condannato in via definitiva per peculato, essendosi appropriato di somme della procedura esecutiva senza l'autorizzazione del giudice. In applicazione del principio di cui in massima, il CNF ha ritenuto congrua la sanzione disciplinare della radiazione*).

Consiglio Nazionale Forense (pres. f.f. Logrieco, rel. Savi), sentenza del 12 settembre 2018, n. 109

radiazione

La radiazione costituisce trattamento sanzionatorio che va adeguato alla gravità della condotta in reiterata violazione dei fondamentali e più cogenti doveri professionali, della totale mancanza di resipiscenza, della pervicacia con la quale l'incolpato ha posto in essere la sua condotta.

Consiglio Nazionale Forense (pres. f.f. Logrieco, rel. Savi), sentenza del 12 settembre 2018, n. 109

corrispondenza riservata

La norma deontologica di cui all'art. 48 cdf (già art. 28 codice previgente) è dettata a salvaguardia del corretto svolgimento dell'attività professionale, con il fine di non consentire che leali rapporti tra colleghi potessero dar luogo a conseguenze negative nello svolgimento della funzione defensionale, specie allorché le comunicazioni ovvero le missive contengano ammissioni o consapevolezze di torti ovvero proposte transattive. Ciò al fine di evitare la mortificazione dei principi di collaborazione che per contro sono alla base dell'attività legale. Di tal chè

il divieto di produrre in giudizio la corrispondenza tra i professionisti contenente proposte transattive assume la valenza di un principio invalicabile di affidabilità e lealtà nei rapporti interprofessionali, quali che siano gli effetti processuali della produzione vietata, in quanto la norma mira a tutelare la riservatezza del mittente e la credibilità del destinatario, nel senso che il primo, quando scrive ad un collega di un proposito transattivo, non deve essere condizionato dal timore che il contenuto del documento possa essere valutato in giudizio contro le ragioni del suo cliente; mentre, il secondo, deve essere portatore di un indispensabile bagaglio di credibilità e lealtà che rappresenta la base del patrimonio di ogni avvocato. La norma, peraltro, non è posta ad esclusiva tutela del legale emittente, ma anche all'attuazione della sostanziale difesa dei clienti che, attraverso la leale coltivazione di ipotesi transattive, possono realizzare una rapida e serena composizione della controversia.

La violazione dell'art. 48 cdf (divieto di produrre o riferire in giudizio la corrispondenza espressamente qualificata come riservata quale che ne sia il contenuto, nonché quella contenente proposte transattive scambiate con i colleghi a prescindere dalla suddetta clausola di riservatezza) costituisce illecito disciplinare, a nulla rilevando in contrario né l'errore di valutazione dell'incolpato sul contenuto della corrispondenza stessa, né l'eventuale irrilevanza della produzione stessa sul convincimento del giudice (*Nel caso di specie, l'incolpato -che aveva prodotto in giudizio una lettera contenente proposte transattive- si era difeso in sede disciplinare eccependo che la produzione era dipesa da un mero errore di valutazione sul contenuto della corrispondenza, che peraltro a suo dire non aveva comunque condizionato la decisione del giudice. In applicazione del principio di cui in massima, il CNF ha rigettato l'eccezione*).

Consiglio Nazionale Forense (pres. f.f. Logrieco, rel. Masi), sentenza del 27 settembre 2018, n. 110

espressioni sconvenienti ed offensive

L'avvocato deve svolgere la propria attività con lealtà e correttezza, non solo nei confronti della parte assistita, ma anche e soprattutto verso l'ordinamento (generale dello Stato e particolare della professione), verso la società, verso i terzi in genere, in quanto i concetti di probità, dignità e decoro costituiscono doveri generali e concetti guida, a cui si ispira ogni regola deontologica, giacché essi rappresentano le necessarie premesse per l'agire degli avvocati.

Nell'ambito della propria attività difensiva, l'avvocato deve e può esporre le ragioni del proprio assistito con ogni rigore utilizzando tutti gli strumenti processuali di cui dispone e ciò massimamente nella fase dell'impugnazione, atto diretto a criticare anche severamente una precedente decisione giudiziale e ciò rappresentando con la maggiore efficacia possibile la carenza di motivazione del provvedimento impugnato. Tuttavia, il diritto della difesa incontra un limite insuperabile nella civile convivenza, nel diritto della controparte o del giudice a non vedersi offeso o ingiuriato: soggetti nei confronti dei quali non devono essere utilizzate espressioni dirette consapevolmente ad insinuare la esistenza di condotte illecite o la violazione del fondamentale dovere di imparzialità, dovendosi mantenere con il giudice un rapporto improntato a dignità e decoro sia con riferimento alla persona del giudicante che al suo operato e alla funzione esercitata.

Consiglio Nazionale Forense (pres. f.f. Salazar, rel. Losurdo), sentenza del 27 settembre 2018, n. 113

formazione continua

L'obbligo di formazione continua sussiste per il solo fatto dell'iscrizione nell'albo e non subisce deroga né attenuazioni nel caso di asserita disorganizzazione amministrativa del proprio studio, conseguente al licenziamento contemporaneo delle segretarie, giacché tale circostanza non rientra tra le ipotesi previste dall'art. 5 Regolamento CNF per la formazione continua 16 luglio 2014, n. 6 come motivo di dispensa.

La partecipazione ad un corso "per acquisire la qualità di mediatore" non assume rilievo ai fini dell'adempimento al dovere di formazione e aggiornamento professionale, non rientrando tale attività tra gli "eventi formativi" e le "attività formative" di cui agli artt. 3 e 4 del Regolamento CNF per la formazione continua 16 luglio 2014, n. 6.

Consiglio Nazionale Forense (pres. Mascherin, rel. Baffa), sentenza del 16 ottobre 2018, n. 116

l'incarico nei confronti dell'ex cliente

Il divieto di assumere l'incarico nei confronti dell'ex cliente (art. 68 cdf, già art. 51 codice previgente), prescinde dalla natura giudiziale o stragiudiziale dell'attività prestata a favore di quest'ultimo, giacché è sufficiente una prestazione professionale nella più ampia definizione di assistenza, così come è irrilevante il motivo per il quale la dismissione del mandato sia avvenuta, ossia per revoca o rinuncia.

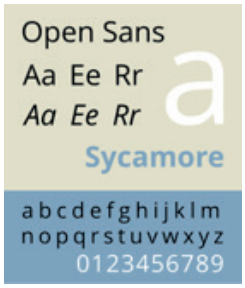
L'avvocato non può né deve assumere un incarico professionale contro una parte già assistita se non dopo il decorso di almeno un biennio dalla cessazione del rapporto professionale (comma 1), ma anche dopo tale termine deve comunque astenersi dall'utilizzare notizie acquisite in ragione del rapporto già esaurito (comma 3). Peraltro, il divieto de quo non è soggetto ad alcun limite temporale se l'oggetto del nuovo incarico non sia estraneo a quello espletato in precedenza (comma 2), ovvero quando dovesse assistere un coniuge o convivente more uxorio contro l'altro dopo averli assistiti congiuntamente in controversie di natura familiare (comma 4), ovvero ancora quando abbia assistito il minore in controversie familiari e poi dovesse assistere uno dei genitori in successive controversie aventi la medesima natura o viceversa (comma 4).

Il precetto deontologico di cui all'art. 68 cdf non consente all'avvocato di assumere incarichi contro ex clienti, a meno che sia decorso un ragionevole periodo di tempo, l'oggetto del nuovo incarico sia estraneo a quello espletato in precedenza e non vi sia possibilità, per il professionista, di utilizzare notizie precedentemente acquisite. Conseguentemente, pur quando non ricorrano nella fattispecie tutte le condizioni innanzi richiamate, il rigido tenore della predetta norma può indubbiamente ritenersi superato allorché il soggetto – alla cui tutela la norma è in parte orientata -, autorizzando espressamente il professionista a non tener conto del divieto, lo libera dal vincolo deontologico impostogli dal precetto.

Consiglio Nazionale Forense (pres. f.f. Logrieco, rel. Baffa), sentenza del 16 ottobre 2018, n. 123

Anno XXVIII numero uno
(ottantunesimo della serie)
febbraio 2019

Questo numero usa il carattere



è un carattere senza grazie disegnato da Steve Matteson e commissionato da Google, utilizzato in alcune sue pagine web, nonché nella sua pubblicità (it.wikipedia.org)

si distingue per l'occhio medio alto, per le forme aperte e un contrasto molto basso. Non ha particolari segni distintivi ma nella sua "neutralità" ha un aspetto fresco e gradevole, oltre a un'eccellente leggibilità (antoniofiligno.com)

in copertina:
Giacomo Balla ("Futurballa") – 1923
pessimismo e ottimismo
GNAM Roma
con intervento redazionale in stile shodo

numerose altre immagini fuori testo di:
Linda Vukai dal progetto Parallel Lands.

www.lindavukaj.com

progetto grafico di **Alessandro Riccomini** - stampa **Cabiria**