

CITTADINANZA DIGITALE E BLOCKCHAIN, UNA INNOVAZIONE LA CUI CONOSCENZA E' STRUMENTO DI FISCAL FITNESS PUBBLICA.

La cittadinanza digitale.

Il concetto di cittadinanza digitale si è fatto strada nell'ultimo decennio.

L'Unione europea ha predisposto un piano per l'eGovernment sin dal periodo 2016-2020¹ a favore della digitalizzazione della Pubblica Amministrazione, da conseguire semplificando e rimodernando i processi interni.

È aumentato, notevolmente, il numero di servizi pubblici online, e sono stati perfezionati e adottati, in molti casi, sistemi di autenticazione sicura in rete: le cosiddette identità digitali – EID.

Tra i principali regolamenti a livello europeo si possono citare il regolamento eIDAS del 2014², e quello del General Data Protection Regulation del 2016³, ma, anche, la Dichiarazione Ministeriale sull'eGovernment di Tallinn⁴ per i principi di inclusività, sicurezza, protezione dei dati personali e principio once-only in esso presenti, nonché, la proposta di revisione del regolamento eIDAS⁵ (regolamento sull'identificazione elettronica e servizi fiduciari).

Si discute, sempre più assiduamente, di digitalizzazione e di eGovernment nel contesto europeo: (v. gli appena citati Government Action Plan 2016-2020, e la Dichiarazione Ministeriale sull'eGovernment di Tallinn (2017)), quali “manifesti europei” che affrontano e asseriscono principi come il “digital by default”, l'inclusività, l'accessibilità, il principio “once-only”, la sicurezza, la trasparenza e l'interoperabilità.

L'idea di eGovernment (o amministrazione digitale) si basa su un netto incremento dell'efficienza, da cui consegue un risparmio per imprese e Pubbliche Amministrazioni, oltreché, maggiore trasparenza.

E, pur se, innovare costa fatica, e richiede tempo, la tecnologia, secondo la strategia europea, non può più essere una barriera, ma deve diventare strumento e valore aggiunto a favore dei cittadini, delle imprese e della P.A.

Esistono, già, diverse tipologie di strumenti: l'identità digitale, la firma elettronica digitale, la PEC, la marca temporale (che certifica la data e l'ora di emissione e che apposta, anche, a file non firmati digitalmente permette di validarli legalmente).

Sono tutti strumenti noti e usati, ormai, nella pratica corrente.

Anche la normativa europea è nota: Il regolamento eIDAS (2014/910/EU)⁶, il regolamento di esecuzione 2015/1501/EU⁷, regolamento 2016/679/EU⁸ e regolamento 2018/1724/EU⁹, il ruolo e i compiti dell' Agenzia dell'Unione europea per la cybersicurezza e il regolamento 2019/881/UE¹⁰, dell' Istituto Europeo per gli Standard nelle Telecomunicazioni (ETSI)¹¹ e dell'Organizzazione Internazionale per la Standardizzazione (ISO)¹².

Norme sviluppate per tracciare una linea comune di raccordo nella complessità degli strumenti digitali in materia di identificazione.

Anche l'Italia si è dotata di organismi e di norme per far fronte alla sfida della trasformazione digitale della Pubblica Amministrazione: esiste, quindi, un'agenzia apposita, l'AgID¹³, con il compito di guidare e supportare questo periodo di transizione, mentre il testo normativo di riferimento è il Codice dell'amministrazione digitale (CAD)¹⁴.

L'obiettivo è teso a pianificare l'attività delle Pubbliche Amministrazioni e i rapporti con altre Pubbliche Amministrazioni e i cittadini o le loro organizzazioni, mediante l'impiego delle tecnologie dell'informazione e della comunicazione, soddisfacendo i principi sopra richiamati di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione tipici dell'apparato amministrativo pubblico.

Alla guida di questo processo è stata prevista la figura del Responsabile per la Transizione al Digitale (RTD), obbligatoria in tutte le amministrazioni.

Per realizzare il suo mandato, l'AgID crea dei piani per l'innovazione e l'informatica nella Pubblica Amministrazione nei quali vengono enunciati i principi chiave per l'avanzamento della trasformazione digitale della Pubblica Amministrazione. Dal "digital by default" al "digital identity only".

L'identità digitale deve essere intuitiva, sicura e permettere, senza eccezioni, l'accesso a tutti i servizi digitali pubblici e privati, l'obiettivo è raggiungere la totale copertura della popolazione.

Ma per far sì che gli utenti privilegino i canali on-line, i servizi pubblici digitali devono lavorare di qualità e di informazione/formazione e sulla user experience, cercando di privilegiare inclusività, interoperabilità e la non frammentazione.

Per quanto riguarda, invece, le piattaforme esse devono essere trasversali e permettere di diminuire la mole di lavoro degli uffici attuando modalità di risparmio in termini di tempo e denaro.

La funzione che diventa prevalente è quella del back-office, che deve stimolare la creazione di ulteriori servizi digitali e la semplificazione dei processi. Vanno appoggiate e migliorate le piattaforme già esistenti, e vanno promosse nuove piattaforme, interconnesse tra loro.

Anche le linee guida non sono mancate, e in ambito di digitalizzazione, viene introdotta e sottolineata la procedura e il valore della "certificazione di processo" che, attraverso la dematerializzazione degli elementi dell'atto, attesta l'uguaglianza dei documenti analogici rispetto ai loro corrispondenti digitali durante tutto il processo di dematerializzazione e ne permette il veloce trasferimento

Questa la prima vera certezza : una comunicazione veloce e aggiornata di dati che si presentano disponibili e pronti all'uso, accelerando l'offerta e la prestazione di servizi e riformulando il rapporto tra Pa e cittadino¹⁵.

Cosa e' la blockchain e come funziona.

È utile, a tal proposito, introdurre subito il concetto di blockchain.

La blockchain è fondamentalmente un database distribuito¹⁶.

Si può pensare a un gigantesco foglio di calcolo globale, che funziona su milioni e milioni di computer, allocati in tutto il mondo.

È distribuito, appunto. È “open source”, quindi chiunque può conoscere il codice sottostante e accedere per vedere cosa è in atto.

È una formula “peer to peer”(tra pari); che non richiede potenti intermediari per autenticare o regolare le transazioni.

Utilizza una crittografia all'avanguardia, che protegge i contenuti delle transazioni.

Può registrare qualsiasi informazione strutturata, non solo chi ha pagato chi, ma anche chi possiede quale terra o quale energia ha acquistato, o quale fonte di energia ha usato. Gli esempi sono infiniti.

Nel caso dell'Internet delle cose, esso viene integrato da un sistema di regolamento blockchain sottostante.

La blockchain è, anche, un database distribuito immutabile e non hackerabile di risorse digitali¹⁷.

“Una piattaforma per la verità ed è una piattaforma per la fiducia”, così viene definita dai molti studiosi di settore.

Le implicazioni sono sbalorditive, non solo per l'industria dei servizi finanziari, ma anche praticamente in ogni aspetto della società.

La maggior parte delle blockchain, più note ad oggi, e tra quelle finanziarie, Bitcoin era la più grande, sono quelle che si chiamano sistemi senza autorizzazione.

Possiamo fare transazioni e soddisfare reciproci bisogni economici, senza sapere chi sia l'altra parte e indipendentemente dalle autorità centrali che autorizzino l'operazione.

Queste blockchain hanno tutte una valuta digitale di qualche tipo ad esse associata, motivo per cui SI parlava, all'inizio del loro avvento, di Bitcoin nello stesso “discorso” della blockchain, in verità la valuta digitale all'interno di una rete di blockchain può essere costituita, anche, da token.

Ma, la blockchain è, in verità, la tecnologia sottostante, e rappresenta la più grande innovazione nell'informatica: l'idea di un database distribuito, in cui si stabilisce “fiducia”, attraverso la collaborazione di massa e si usa un codice intelligente, piuttosto che l'autorizzazione di una potente istituzione, per l'autenticazione e l'insediamento.

La blockchain è definita, anche, come un registro aperto che offre decentramento alle parti, e garantisce trasparenza, immutabilità e sicurezza¹⁸.

Ha molte caratteristiche tra le quali quella di essere un registro distribuito, P2P (peer to peer, cioè tra pari) e permanente.

Il termine Blockchain è stato introdotto per la prima volta nel white paper di Bitcoin nel 2009 da Satoshi Nakamoto, autore (o autori), sconosciuto alle cronache e la cui identità è rimasta non rivelata.

Ma, la blockchain di Bitcoin è stata solo la prima di tante.

Come funziona?

Il funzionamento di una blockchain è semplice e si può, in via generale, rappresentare come segue: poiché si tratta di una rete peer-to-peer, si comincia con un utente che deve avviare una transazione. Una volta fatta, un blocco viene allocato a detta transazione. Il blocco della transazione viene anche trasmesso alla rete e tutti i nodi della rete ottengono le stesse informazioni. Il blocco viene quindi estratto e convalidato. Viene anche aggiunto alla catena di blocchi esistenti, a seguito di una transazione riuscita.

Il meccanismo attiene alla registrazione su tutti i nodi dei medesimi dati, perché ogni nodo contiene le informazioni del precedente e così via a ritroso. Ciò garantisce, anche, la cosiddetta tracciabilità dei dati e delle transazioni.

La tecnologia Blockchain è ricca di funzionalità, ed è, anche, estremamente vantaggiosa e consente all'utente di effettuare un regolamento rapido delle proprie movimentazioni economiche e finanziarie, rispetto ai metodi tradizionali.

È immutabile e più sicura.

Rispetto a una rete tradizionale, la tecnologia blockchain è più efficiente e ha una capacità di rete migliorata.

Il decentramento integrato, consente, inoltre, la costruzione di una blockchain condivisa e distribuita. Ciò la rende idonea agli usi pubblici.

Blockchain vs database

La blockchain è un a rete decentralizzata che memorizza anche i dati¹⁹.

Tuttavia, è diversa dai database e si possono fare dei confronti tra blockchain e database.

Le quattro categorie in cui differiscono includono i concetti di accesso alla scrittura, il costo, l'integrità e la fiducia.

La differenza principale è, ovviamente, e sempre, l'assenza di un'autorità centralizzata, oltreché, la certezza che i dati trascritti su blockchain sono immutabili, il che a sua volta fornisce integrità.

Il database, invece, offre un funzionamento CRUD = Create – Read – Update – Delete²⁰, che tradotto significa: Creazione – Lettura – Aggiornamento – Rimozione; che sono le quattro operazioni basilari della gestione persistente dei dati, e che, appunto, ammette la loro modifica.

Al funzionamento della blockchain contribuiscono diversi tipi di token, che includono token di valuta, asset, utility e equity. Sono elementi indispensabili del sistema blockchain e possono essere definiti in via generale come una sorta di gettone virtuale, che può essere usato come moneta virtuale, ma che è basato su una blockchain esistente. Non sono, quindi, delle semplici valute digitali, ma la rappresentazione di un bene digitale.

Come con qualsiasi tecnologia emergente, la blockchain deve affrontare sfide e ostacoli alla sua adozione e minacce da cui difendersi.

Anche una piattaforma più ampia non può sempre prevenire gli hack!

Un, ormai, non più recente "attacco del 51%" all'exchange di token Ethereum Classic, ha mostrato, infatti, perché anche la blockchain non è, totalmente, impermeabile a giochi criminali, restando, pur sempre, lo strumento più sicuro, ad oggi disponibile.

Il caso è quello di un attacco del 51% che si riferisce a un cattivo attore (o più cattivi autori), che ottiene il controllo della maggior parte delle CPU (Central Process Unit), in un "pool di mining di criptovalute".

Tali attacchi sono generalmente limitati a blockchain più piccole, con meno nodi, che sono più suscettibili al controllo di una singola fonte, in base al meccanismo di consenso c.d. Proof of Work (PoW), tuttavia, ciò se pur possibile, resta una ipotesi difficile da praticare e comporta uno sforzo in termini di oneri grandissimi, anche, per i malintenzionati.

Sicché, pur se le reti blockchain sono tendenzialmente sicure, le applicazioni in esecuzione su di esse, secondo Bruce Schneier, crittografo ed esperto di sicurezza, sono migliorabili in base alla loro diffusione.

Anche se questi progressi sono tutti in cammino, le industrie stanno, comunque, aumentando i progetti pilota e le implementazioni in tempo reale di blockchain, per settori come la spedizione, il fintech, la sanità, l'energia e l'immobiliare o la supplychain per il commercio internazionale.

Con la tecnologia blockchain i passaggi vengono ridotti al minimo indispensabile, così come gli errori o le frodi possibili.

Egovernment e intelligenza artificiale, blockchain e fisco, dal caso "Estonia" a "Roma".

Tra i Paesi europei emerge che i più performanti in digitalizzazione sono Malta, Estonia ed Austria, seguiti da Lettonia, Lituania e Finlandia.

Tuttavia è l'Estonia il Paese dei servizi pubblici digitali (eServices)²¹ È anche una delle nazioni più connesse del mondo per la diffusione di internet e della partecipazione dei cittadini alla vita on-line. L'uso di internet è previsto come un diritto dai cittadini e la connessione WI_FI è per lo più gratuita ovunque.

Tutti i servizi disponibili sono accessibili tramite eID nell'ottica di parità tra autenticazione on-line e di persona. La realtà si è tradotta in vincente grazie alla sinergia tra Stato, settore ICT e la popolazione, che si è rivelata pronta ad accogliere i cambiamenti tecnologici.

Oltre ad una buona quantità di investimenti dedicati, certamente hanno avuto il loro peso effetti conseguenti ad un orientamento culturale di fiducia che gli estoni condividono nei confronti del loro governo. Ma la fiducia è stata implementata e direzionata da anni di informazione e formazione digitali proposta a tutti i cittadini, sin dalle scuole dell'infanzia.

L'apparato che supporta la digitalizzazione dell'Estonia, si chiama X-Road²², e consiste in un sistema virtuale sicuro, creato per lo scambio di dati in ambito di servizi elettronici, e per questo collega tra loro i vari database presenti sul territorio nazionale, assicurando una comunicazione protetta secondo il principio dell'interoperabilità. La sicurezza viene garantita da dati criptati o autenticati dall'utente.

La diffusione dei servizi digitali è derivata dalla qualità del sistema di identità digitale dell'Estonia, che vanta la prerogativa di essere uno tra i più sviluppati del mondo. Ma tutto inizia dalle banche dati.

- **E-Governance ed efficienza fiscale.**

L'intelligenza artificiale e la tecnologia blockchain possono portare sicuramente benefici per l'avanzamento dell'eGovernment²³, come l'aumento dei servizi offerti, la semplificazione dei processi burocratici, la trasparenza e immodificabilità delle informazioni, l'affidabilità e la sicurezza dei dati, e infine la riduzione dei costi.

Le sfide sul loro uso in ambito di eGovernment riguardano la scalabilità del modello, la possibile fuga di dati, la distorsioni delle transazioni dovute all'acquisizione illegale dei nodi da parte di utenti terzi.

Ma tutte le vulnerabilità di sistema si risolvono se si rende ampio il network o il grande gruppo di nodi della catena di blockchain.

Non si manca di sottolineare il rischio di incidenti e di potenziali attacchi hacker che possono mettere a rischio i sistemi, ma si evidenzia come molti degli errori di sistema (hardware e software) siano causati dall'errore umano, che si può prevenire con una adeguata preparazione digitale, che è il primo degli obiettivi da realizzare e prefiggere per la formazione innanzitutto del personale già esistente all'interno degli apparati amministrativi statali.

E' di tutta evidenza la portata del cambiamento e i vantaggi dell'uso derivanti da una prova certa dell'identità in rete.

Un'unica identità digitale, utile e necessaria, per accedere a qualsiasi servizio della Pubblica Amministrazione è un progetto in atto da circa dieci anni nei diversi Stati europei.

L'identificazione digitale dei cittadini, e delle entità giuridiche, e un sistema di interscambio di dati digitali associato a una rete di applicazioni, e costituiscono, tutti insieme, una sorta di web-amministrativo sviluppato per finalità di interesse pubblico e privato.

Grazie all'e-management fiscale²⁴ il risultato è una piattaforma multiuso e multi servizi, gestita dall'Amministrazione Finanziaria e capace di garantire che il 95% dei documenti di rilevanza fiscale sia quotidianamente archiviato online.

È da un decennio, infatti, che si guarda alle Digital Republic come ad un esempio da seguire.

In questo periodo ancora di più, considerando i fondi che da più parti si stanno mettendo in campo per la digitalizzazione, l'informatizzazione e la sicurezza.

Uno dei motivi per cui nell'era moderna si spinge e si deve spingere verso un utilizzo sicuro e consapevole della tecnologia, è la riduzione di processi burocratici obsoleti. L'accesso a internet, è un diritto fondamentale. E' la base per costruire strutture ed infrastrutture tecnologiche effettivamente fruibili da tutta la popolazione.

Il primo paese a far funzionare la macchina digitale, è stata l'Estonia, appunto, munendosi di una piattaforma che permette ai vari server di comunicare tra loro attraverso la blockchain.

Circa 500 milioni sono gli scambi di dati su X road, sistema che l'Estonia condivide con la vicina Finlandia per consentire la massima fruibilità ai cittadini di entrambi i paesi.

Un sistema che ha innalzato fortemente il livello di sicurezza di scambio dati.

Creare la stessa risorsa nel nostro paese sarà la vera rivoluzione ed è assolutamente possibile oggi.

Quasi totalmente in digitale, in Estonia vanno anche le imprese private, semplificando i processi e promuovendo la nascita di start up in ambito informatico.

Il sistema paese, incoraggia a tal proposito, anche, investitori esteri a fare impresa in Estonia, con il programma E-Residency²⁵, attraverso il quale chiunque può avviare un'azienda, anche se non residente secondo il regime legale e fiscale estone.

Più informatizzazione, significa anche maggiori entrate tributarie.

Oltre a risparmiare tempo, la digitalizzazione ha il vantaggio di rafforzare l'abilità dell'Amministrazione finanziaria sia nel recupero dell'evasione che nella raccolta e tracciabilità del gettito atteso da imposte e tasse.

L'efficienza nella raccolta dei tributi estone è stata classificata tra le migliori dell'Ocse, e anche l'Italia può seguire lo stesso esempio.

Le riforme fiscali incontrano lo strumento digitale!

Nel paese estone, la *Tax and Customs Board (ETCB)*²⁶,organo parzialmente assimilabile al nostro Ministero delle Finanze, ha spostato le sue procedure fiscali online e ha reso digitale l'analisi dei dati amministrativi di rilevanza fiscale.

I micro-dati ricavati dai pagamenti dei contribuenti e dagli scambi finanziari, uniti ai dati provenienti da altri dipartimenti governativi, sono utilizzati per produrre profili di rischio e liste selettive e di obiettivi.

I micro-dati sono, anche, usati per evidenziare le potenziali frodi intracomunitarie, fenomeno che costituisce un rischio endemico per l'Estonia come membro dell'Ue, ma che è presente come problema comune di tutti i paesi appartenenti all'UE.

Il Dipartimento di *intelligence* del fisco estone utilizza direttamente dati dei contribuenti per identificare i rischi nei crediti Iva e per mettere in risalto le cosiddette popolazioni di *contribuenti anomali*, soggetti i cui profili, provenienti da più fonti, sembrano non combaciare o essere persino in aperto contrasto o disallineamento, con i parametri di congruità reddituale stabiliti.

In questo ambito, i funzionari fiscali utilizzano, anche, un'analisi longitudinale dei dati per identificare il comportamento ad alto rischio o anomalo nel tempo (ad esempio, aggiustamenti online rapidamente ripetuti da parte dei contribuenti che riducono o invertono sistematicamente le proprie passività).

Questo approccio, aperto all'analisi dei rischi, consente alle Entrate estoni di identificare e contrastare più rapidamente le minacce di evasione o elusioni che via via emergono o si palesano.

Sebbene l'Italia si stia muovendo sulla stessa linea, l'operatività digitale non è ancora stata eletta a sistema, ma il segnale è incoraggiante stando alle disposizioni previste dall'art. 5, comma 5 del DM 28 giugno 2022²⁷, pubblicato di recente sul sito dell'Agenzia delle Entrate italiana, che prevede accertamenti digitalizzati con l'uso della Intelligenza artificiale e con motivazione rafforzata a tutela dei contribuenti sottoposti a verifica.

Tuttavia, a livello italiano, le disposizioni e le applicazioni ma, soprattutto, le interpretazioni della giurisprudenza non sono univoche. Una bella pronuncia, da tenere presente ad esempio, è quella recente del Consiglio di Stato, che con la sentenza n. 2270/2019, rifacendosi anche ad orientamenti eurocomunitari conformi, dichiara che l'uso della intelligenza artificiale nei processi amministrativi non è vietato ma impone, e ciò a pena di nullità, che siano resi espliciti e chiari i linguaggi e le procedure anche algoritmiche seguite e il loro processo di funzionamento.

Ovviamente e comprensibilmente tale indirizzo è posto in un'ottica di garanzia del contribuente, che per difendersi adeguatamente dovrà essere edotto dei rischi fiscali contestati e delle procedure che tali contestazioni hanno determinato.

Ancora a proposito di digitalizzazione, sin dal 2014, nel Paese estone, nostro esempio di riferimento, è stato introdotto l'onere della fatturazione elettronica, con il deposito elettronico obbligatorio a livello di transazione per l'Iva e l'abbinamento automatico dei dati per combattere le frodi.

La misura ha reso obbligatoria, per i contribuenti, le fatture di acquisto e di vendita tramite e-file con le relative dichiarazioni Iva. Ciò ha consentito all'Amministrazione di abbinare automaticamente le richieste di credito d'imposta in entrata con i pagamenti delle imposte in uscita e di esaminare le discrepanze e gli elementi non corrispondenti.

Si tratta di una misura talmente valida, che anche l'Italia l'ha introdotta da qualche anno²⁸ e che, pur se inizialmente ha comportato oneri amministrativi elevati, ha consentito il primo vero momento di allineamento dei dati incrociati e tracciabili dei contribuenti a disposizione dell'Agenzia Entrate.

Gi iniziali costi e svantaggi sono stati, ulteriormente, attenuati dall'amministrazione fiscale estone effettuando il *profiling* di rischio delle transazioni prima della fase di abbinamento dei dati, in modo da verificare solo le fatture a rischio più elevato.

Da quando è stata introdotta la misura, il divario di conformità in Estonia è sceso ad uno dei livelli più bassi di *Vat-gap* tra i paesi Ue.

A questo punto sostenere che l'Italia abbia iniziato il percorso non basta, resta un paese indietro nella utilizzazione globale di banche dati sempre aggiornate e interoperabili tra loro, che viaggiano su piattaforme connesse e in uso ad operatori forniti di conoscenze adeguate.

Il percorso di riforma e di preparazione digitale delle risorse umane impegnate agevolerebbe di gran lunga sia l'interoperabilità dei sistemi che l'aggiornamento dei dati disponibili.

Opportunità future, il ruolo della politica nella realizzazione della cittadinanza e della fiscalità digitale.

Al maturare della tecnologia, i problemi di capacità vengono affrontati e anche le leggi si aggiornano, anche, se con più ritardo.

Ci si può aspettare di vedere catene di approvvigionamento commerciali globali complete che utilizzano blockchain, con la partecipazione delle autorità per monitorare le transazioni e il rispetto delle regole di origine, delle dichiarazioni doganali e dei dazi e con regole di pagamento e sanzioni perfettamente applicate tramite gli smart contract.

La combinazione della blockchain con l'IoT (Internet of things), consentirà ai produttori di tracciare e rintracciare lotti di prodotti, per gestire il rischio di importazioni grigie, all'interno delle loro reti di distribuzione, e dimostrare una buona governance aziendale.

Bisogna precisare che, già oggi, la maggior parte delle attuali piattaforme e soluzioni blockchain sono in grado di convalidare le transazioni in tempo reale.

E con l'aumento della capacità e della velocità di elaborazione, si apriranno nuove applicazioni e opportunità per l'implementazione della blockchain.

Le aziende che esplorano le applicazioni blockchain iniziano in piccolo, con un focus su un paese o processo, e imparando da questi esperimenti, hanno compreso come implementarli in modo più ampio.

Allo stesso tempo, tutti gli interessati stanno affrontando i problemi legati alla blockchain presso i tribunali, per ottenere chiarimenti con verdetti vincolanti, su cui fare affidamento in futuro, ovviamente, contestualizzando i diversi settori di competenze. Taluni campi del diritto, infatti, si prestano alle nuove tecnologie, maggiormente, rispetto ad altri, più sensibili alla interpretazione, del giudice.

Lo Stato di Malta, per esempio, è recentemente diventato il primo paese al mondo ad approvare leggi²⁹, che stabiliscono un quadro normativo per blockchain, criptovalute e tecnologia di contabilità distribuita, ma passi da gigante hanno fatto, anche, i Paesi Europei, e fra questi l'Italia con il compromesso di non soffocare l'innovazione tecnologica e le sue performance potenziali, ma tentando, regolamentazioni capaci di prevenire frodi a tutela del cittadino- consumatore.

Nel tempo, saranno necessari il coordinamento e la collaborazione internazionali per facilitare un maggiore utilizzo della blockchain, nel gestire le catene di approvvigionamento del commercio globale e altri usi transfrontalieri della tecnologia, così come sarà necessario uniformare i regolamenti internazionali, anche, legati al mondo finanziario, al fine di mantenere la tracciabilità dei movimenti di capitale e di prevenzioni da usi impropri, da parte di organizzazioni criminali.

È un'opera che, lentamente, è già cominciata e che non si fermerà dal proseguire.

Sfide future

La maggiore automazione dell'Amministrazione fiscale senz'altro presenta anche nuovi rischi.

La registrazione e il deposito online potrebbero consentire a potenziali truffatori fiscali di creare "entità" a costi bassi e di generare rapidamente dichiarazioni e richieste online senza necessità di presenza fisica o aziendale.

E il sistema potrebbe, anche, permettere di generare crediti con un basso rischio di individuazione, presentando più richieste di valori diversi e diverse caratteristiche, al fine di testare i parametri dei profili di rischio a disposizione della apparato amministrativo, riducendo i rischi d'incorrere in una verifica.

A tal proposito, certamente, è la sicurezza informatica che dovrà crescere e realizzare la prevenzione e l'individuazione di violazioni.

Costruire *firewall* contro i cyber-attacchi come primo passo per anticipare le minacce future di eventuali attori maliziosi e tutto ciò può essere facilitato creando una rete di informazioni condivise sulle vulnerabilità tra agenzie governative e aziende private.

Ma la forza del programma è, e sarà, la cyber security awareness³⁰ (consapevolezza della sicurezza informatica nel cyber) da parte del personale addetto, che va adeguatamente ed efficientemente preparato e costantemente aggiornato su procedure e modalità di attacchi e di possibili incidenti informatici.

La risposta sta nello spingere i Paesi a rafforzare la sicurezza dei dati e a condividerli a livello globale oltretutto nell'implementare un sistema avanzato di identità digitale per l'autenticazione degli utenti.

Per questo, oggi, la carta di identificazione digitale, che in Estonia utilizza la tecnologia *blockchain*, per la sicurezza e il Governo, prevede di ospitare i dati di backup in un mondo virtuale a prova di cyber.

Tuttavia, anche in Italia, gli strumenti ci sono (vedi lo SPID, la firma digitale, la Pec, e la sua proposta di regolamento tecnico per un servizio certificato Pec vs REM³¹), e ci sono le professionalità idonee ad individuare il percorso e reindirizzare i processi e ciò sia a livello nazionale che locale.

È nata, da poco, l'INAD, Indice nazionale dei Domicili Digitali, dove i cittadini registreranno la loro Pec e potranno ricevere tutte le comunicazioni ufficiali che li riguardano, da parte della Pubblica Amministrazione.

INAD nasce dalla collaborazione fra Agid e il Dipartimento per la trasformazione digitale della Presidenza del Consiglio, Infocamere e le società delle Camere di Commercio per la innovazione digitale. Partirà il 6 luglio 2023 e sarà liberamente consultabile.

È un passo avanti nella digitalizzazione del sistema Paese italiano che tende a valorizzare, anche, la semplificazione dei rapporti tra tutti gli utenti interessati.

La decisione, quindi, per guardare il fiume è solo politica, le opportunità i vantaggi sono così evidenti che ora è il tempo di una svolta del sistema paese per intero, che non può più attendere.

Bibliografia e sitografia

¹ <https://eur-lex.europa.eu/IT/legal-content/summary/accelerating-the-digital-transformation-of-governments-in-the-eu-2016-2020-action-plan.html>.

² [https://www.agid.gov.it/it/piattaforme/eidas#:~:text=Il%20Regolamento%20eIDAS%20\(electronic%20IDentification,identificazione%20elettronica%20degli%20stati%20membri](https://www.agid.gov.it/it/piattaforme/eidas#:~:text=Il%20Regolamento%20eIDAS%20(electronic%20IDentification,identificazione%20elettronica%20degli%20stati%20membri).

³ <https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html>.

⁴ <https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration>.

⁵ <https://digital-strategy.ec.europa.eu/it/policies/eidas-regulation>

<https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52021PC0281>

⁶ <https://www.agid.gov.it/it/piattaforme/eidas>.

⁷ REGOLAMENTO DI ESECUZIONE (UE) 2015/1501 DELLA COMMISSIONE dell'8 settembre 2015 relativo al quadro di interoperabilità di cui all'articolo 12, paragrafo 8, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

⁸ [https://eur-lex.europa.eu/IT/legal-content/summary/general-data-protection-regulation-gdpr.html#:~:text=Regolamento%20\(UE\)%202016%202016%20del%20Parlamento%20europeo%20e%20del,GU%20L%20119%20del%204.5](https://eur-lex.europa.eu/IT/legal-content/summary/general-data-protection-regulation-gdpr.html#:~:text=Regolamento%20(UE)%202016%202016%20del%20Parlamento%20europeo%20e%20del,GU%20L%20119%20del%204.5)

⁹ <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R1724&from=IT>.

¹⁰ <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019R0891>.

¹¹ <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019R0891>.

¹² <https://www.iso.org/home.html>.

¹³ <https://www.agid.gov.it/>.

¹⁴ <https://www.agid.gov.it/it/agenzia/strategia-quadro-normativo/codice-amministrazione-digitale>.

¹⁵ Paterson, M. (2015), "Embracing the 9 themes of digital citizenship", EdTech [online] at <https://edtechmagazine.com/k12/article/2015/09/embracing-9-themes-digital-citizenship>, accessed on 25 April 2019.

Reynolds L. and Scott R. (2016), "Digital citizens: countering extremism online" (London: Demos).

¹⁶ Daniel Drescher, *Blockchain basics*, Germany, Apress, 2017.

Murray-Rust, D., Elsdon, C., Nissen, B., Tallyn, E., Pschetz, L., & Speed, C. (2022). *Blockchain and Beyond: Understanding Blockchains through Prototypes and Public Engagement*. TOCHI. Retrieved from <https://arxiv.org/abs/2112.11891>.

Bruccoleri M., *Introduzione alla blockchain e agli smart contract*.

-
- ¹⁷ Don Tapscott, Alex Tapscott, *Blockchain revolution*, New York, Portfolio Penguin, 2016.
- Murray-Rust, D., Elsdon, C., Nissen, B., Tallyn, E., Pschetz, L., & Speed, C. (2022). *Blockchain and Beyond: Understanding Blockchains through Prototypes and Public Engagement*. TOCHI. Retrieved from <https://arxiv.org/abs/2112.11891>.
- Nicola Attico, *Blockchain, guida all'ecosistema*, Milano, Guerini Next, 2018.
- ¹⁸ Gianni, R., Mehropouya, H., Murray-Rust, D., Nissen, B., Oosthuizen, S., Speed, C., & Symons, K. (2017). *FinBook: Literary Content as Digital Commodity*. In M. Garrett, N. Jones, R. Catlow, & S. Skinner (Eds.), *Artists Re: Thinking the Blockchain* (pp. 25–32). United Kingdom: Liverpool University Press.
- Murray-Rust, D., Elsdon, C., Nissen, B., Tallyn, E., Pschetz, L., & Speed, C. (2022). *Blockchain and Beyond: Understanding Blockchains through Prototypes and Public Engagement*. TOCHI. Retrieved from <https://arxiv.org/abs/2112.11891>.
- Nicola Attico, *Blockchain, guida all'ecosistema*, Milano, Guerini Next, 2018.
- ¹⁹ Rauchs M. et al. (2018), "Distributed ledger technology system: a conceptual framework (Cambridge Centre for Alternative Finance, University of Cambridge).
- Zheng, Z. et al. (2017), "An Overview of Blockchain Technology: architecture, Consensus and Future Trends", at https://www.researchgat.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends, accessed on 25 April 2019.
- Massimo Di Piero (2017). *What is the Blockchain?* DePaul University.
- ²⁰ <https://appmaster.io/it/blog/operazioni-crudiste-che-cose-il-crudismo>
- ²¹ <https://www.propositionmanagementsearch.com/insight/il-paese-piu-digitalizzato-al-mondo-lestonia-o-meglio-lestonia>
- ²² <https://e-estonia.com/solutions/interoperability-services/x-road/>
- McCullagh, K. (2017), "Cities are about to change forever. Here are 3 key decisions they must make, Fast CoDesign", 05 May, available from <https://www.fastcodesign.com/90123848/cities-are-about-to-change-forever-here-are-3-key-decisions-they-must-make>.
- ²³ <https://www.ibm.com/it-it/topics/identity-access-management>
- McLean, A. (2018), *E-estonia: what is all the fuss about?* ZDNet [online] at <https://www.zdnet.com/article/e-estonia-what-is-all-the-fuss-about/>, accessed on April 2019.
- E-Estonia (2017), *Estonia's I-voting: more secure, more popular* [online] at <https://e-estonia.com/estonias-i-voting-more-popular-more-secure/>, (accessed on 27 April 2019).
- E-Estonia (2019), *E-Schoolbag* [online] at <https://e-estonia.com/solution/education/e-schoolbag/>. (accessed on 27 April 2019).
- ²⁴ <https://e-estonia.com/programme/e-government/>
- ²⁵ Kotka, T. et. Al. (2015), *Estonian e-residency: redefining the nation-state in the digital era* Oxford: Cyber Studies Program Working Paper series No 3, University of Oxford.
- Sullivan C. and Burger E. (2017), "E-residency and blockchain Computer Law and Security Report 33".
- ²⁶ <https://www.emta.ee/en>
- ²⁷ <https://www.gazzettaufficiale.it/eli/id/2022/07/26/22A04210/sg>
- ²⁸ <https://www.mef.gov.it/focus/1-gennaio-2019-la-fattura-diventa-elettronica-00001/#:~:text=La%20e%2Dfattura%20viene%20predisposta,dalla%20Legge%20di%20Bilancio%202018>
- ²⁹ <https://www.maltabusiness.it/la-legislazione-blockchain-al-mondo-sara-malta/>
- ³⁰ <https://www.cybersecurity360.it/nuove-minacce/rapporto-clusit-2021-14-di-attacchi-di-spionaggio-cyber-nel-mirino-i-vaccini-covid-19/>.
- Bruccoleri M., *Cyber security awareness*.
<https://www.twt.it/blog/sicurezza-informatica/cybersecurity-in-italia-la-fotografia-dellosservatorio-del-politecnico-di-milano/>.
- Ogun, *Terrorist Use of cyberspace and cyber terrorism, New Challenges and Responses*, IOS Press, Amsterdam, 2020.
<https://www.canada.ca/en/communications-security/news/2022/09/cyber-security-awareness-month-2022.html>
- ³¹ <https://www.agendadigitale.eu/documenti/verso-una-pec-europea-ecco-come-funzionano-il-modello-rem-e-il-sistema-e-delivery/>

Palermo, li 16.06.2023

Avv. Prof. Maria Bruccoleri