

Architetture abilitanti per servizi evoluti in ambito supply chain: Il progetto SCALES

SCALES - Supply Chain Architecture Leading to Enhanced Services 2018-IT-IA-0053 è un progetto co-finanziato dalla call eInvoicing 2018 del programma Connecting Europe Facility (CEF)

UNINFO

La presente pubblicazione è stata co-finanziata dalla call eInvoicing 2018 del programma Connecting Europe Facility (CEF) nell'ambito del Progetto SCALES 2018-IT-IA-0053.

Redattori: Andrea Caccia (UNINFO) e Daniele Tumietto (UNINFO), con il contributo di Alessandro Mastromatteo e Matilde Ratti.

Al documento hanno contribuito gli esperti delle Commissioni UNI/CT 522 “eBusiness e servizi finanziari” e UNI/CT 523 “Blockchain e tecnologie per la gestione distribuita dei registri elettronici (distributed ledger)” ed i partner del progetto SCALES: AgID, UNINFO, Infocert, Polimi - Politecnico di Milano, Consorzio Dafne.

SOMMARIO

1	Premessa	4
2	Il progetto SCALES - Supply Chain Architecture Leading to Enhanced Services.....	6
2.1	Cosa è SCALES?	6
3	Una panoramica su Blockchain e tecnologie a registro distribuito (DLT).....	10
3.1	L'evoluzione della tecnologia: passato e presente.....	10
3.2	I pilastri dell'Internet del valore: alcune definizioni e caratteristiche tecniche.....	11
3.3	I tipi di utilizzo di Blockchain e modello DLT-RegRep.....	13
3.4	Modello generale di funzionamento di SCALES.....	16
4	La ricerca condotta dal Politecnico di Milano Osservatorio Digitale B2B	17
4.1	Il ruolo dell'Osservatorio digitale B2b	17
4.2	I principali risultati.....	17
4.3	Il nuovo quadro di riferimento e la tabella di marcia delle attività.....	19
4.4	Un ulteriore passo avanti: gli strumenti di finanziamento della supply chain	21
5	Regolamento (EU) 2016/679 e Prassi di Riferimento UNI/PdR 43:2018.....	22
5.1	Il Regolamento (EU) 2016/679.....	22
5.2	Prassi di Riferimento UNI/PdR 43:2018	28
6	Allegati	30
6.1	Termini & definizioni:	30
6.2	Fonti da tenere in considerazione.....	30
6.3	Norme tecniche e raccomandazioni internazionali	31
6.4	La Direttiva 2014/55/UE sulla fatturazione elettronica negli appalti pubblici	32
6.5	Lo standard europeo sulla fattura elettronica EN 16931:2017.....	36
6.6	I servizi offerti dall'Agenzia delle entrate per emissione, archiviazione fatture elettroniche.....	37

1 PREMESSA

Il progetto SCALES 2018-IT-IA-0053 è un progetto finanziato dalla call “eInvoicing 2018” del programma Connecting Europe Facility (CEF) a cui partecipano AgID - Agenzia per l'Italia Digitale, coordinatore del consorzio misto pubblico/privato composto da UNINFO Politecnico di Milano, InfoCert e Consorzio DAFNE.

Obiettivo di SCALES è la progettazione e realizzazione di un'architettura per la Supply Chain digitale abilitante servizi a valore aggiunto destinati alle imprese e alle pubbliche amministrazioni, per questo implementa dal punto di vista logico:

- il modello DLT-RegRep (Registro–Repository) e
- il principio Once only,

creando un ecosistema dei dati che agevola la relazione tra clienti, fornitori, autorità di controllo e soggetti finanziari e abilitando inoltre lo sviluppo di servizi a valore aggiunto (VAS).

Nel caso d'uso della fattura elettronica, il fornitore non invia la fattura, ma la mette a disposizione del cliente e delle autorità di controllo sul proprio nodo SCALES.

L'architettura SCALES adotta tecnologie basate su registri distribuiti (Distributed Ledger Technologies, DLT) ed è progettata in ottica multi-chain in modo da dipendere meno possibile da specifiche implementazioni DLT. Con il modello realizzato si garantisce che solo il soggetto autorizzato ha accesso al documento o a un determinato subset di metadati. Il titolare ha il completo controllo di chi accede ai dati e per quale motivo, oltre ad avere la certezza dell'identità del soggetto che vi accede.

Il modello presenta vantaggi in termini di performance, scalabilità, protezione dei dati.

Il modello SCALES presenta numerosi vantaggi in termini di:

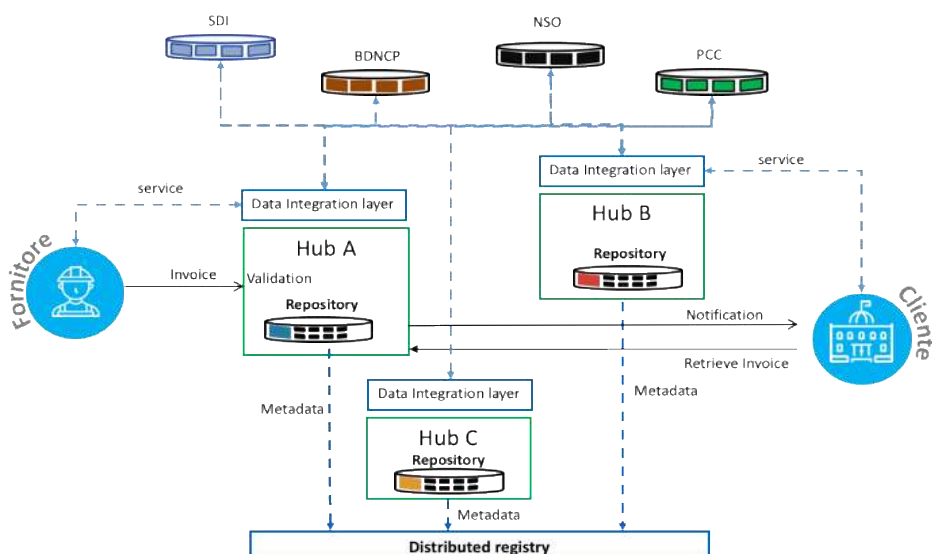
- performance,
- scalabilità,
- protezione dei dati.

L'architettura SCALES, infatti, è stata progettata con specifica attenzione riguardo al trattamento dei dati personali e la conformità al Regolamento 679/2016/EU, il cosiddetto regolamento GDPR.

Particolare analisi ed attenzione è stata posta al ciclo dell'ordine e, in particolare, sulla fatturazione elettronica vista in chiave transnazionale e quindi basata sullo standard di fattura elettronica europea definito dalla EN 16931-1:2017.

È stato anche sviluppato un caso d'uso verticale in ambito sanitario, con coinvolgimento delle aziende del settore farmaceutico, dei distributori e dei depositari.

L'unicità dell'oggetto-documento fattura elettronica è garantita a livello logico, cioè sia seller che buyer sono entrambi presenti in SCALES e accedono al medesimo oggetto, ed ai suoi aggiornamenti a conseguenza dell'intervento dei VAS nel processo.

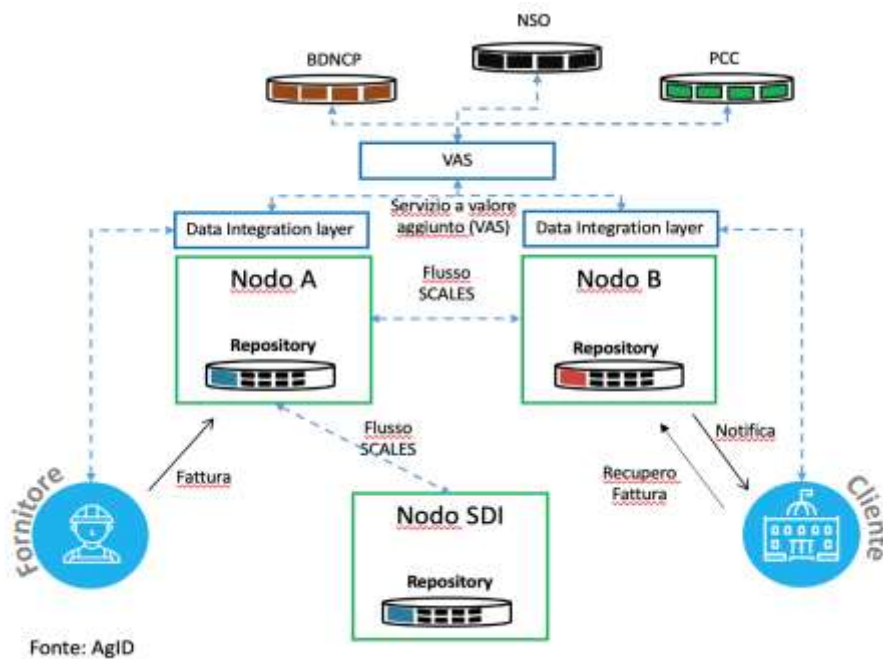


Architettura logica di partenza del progetto SCALES

Infine, SCALES è stata disegnata per permettere anche l'integrazione di sistemi di controllo e monitoraggio quali:

- Sistema di Intercambio (SDI),
- Piattaforma Certificazione Crediti (PCC),
- Banca Dati Nazionale Contratti Pubblici (BDNCP),
- Nodo di Smistamento degli Ordini di acquisto delle amministrazioni pubbliche (NSO),

quali fornitori di servizi a valore aggiunto (VAS) che possono anche non partecipare alla rete con un proprio nodo, ma secondo il seguente schema logico



Schema logico di SCALES

2 IL PROGETTO SCALES - SUPPLY CHAIN ARCHITECTURE LEADING TO ENHANCED SERVICES

2.1 COSA È SCALES?

L'obiettivo di SCALES è la progettazione e realizzazione di un'architettura per la Supply Chain digitale che sia abilitante di servizi a valore aggiunto (VAS) destinati alle imprese e alle pubbliche amministrazioni.

L'architettura SCALES adotta tecnologie a registri distribuiti (DLT) ed è progettata in ottica multi-chain, adottando soluzioni conformi al trattamento dei dati personali ed al Regolamento (UE) 2016/679 (GDPR).

Particolare analisi ed attenzione è stata posta:

- al ciclo dell'ordine,
- alla fatturazione elettronica, in ottica transnazionale,
- all'adozione dello standard di fattura elettronica europea EN 16931-1:2017.

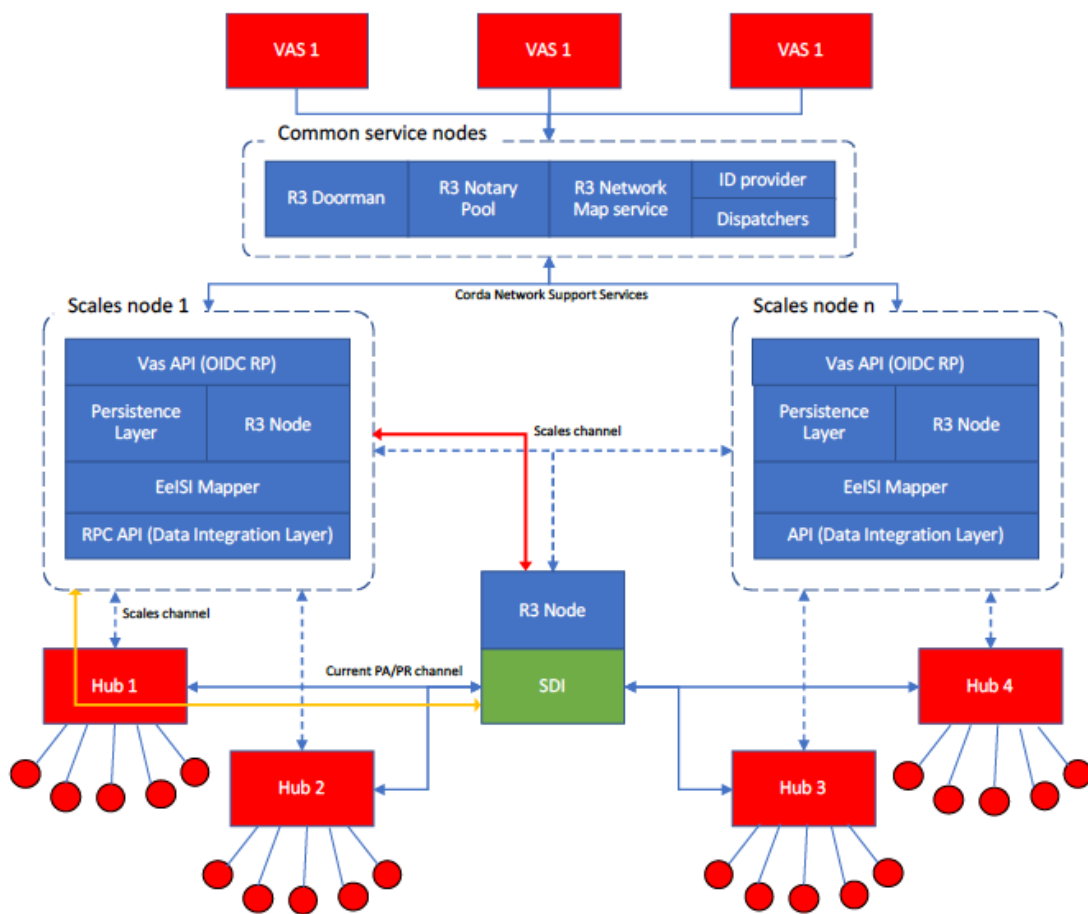
È stato sviluppato un caso d'uso verticale in ambito sanitario, con coinvolgimento delle aziende del settore farmaceutico, dei distributori e dei depositari.

La fattura elettronica è considerata come unico documento a livello logico, quindi seller e buyer entrambi presenti in SCALES accedono al medesimo dato, ed ai suoi aggiornamenti, conseguenti all'interazione coi servizi a valore aggiunto VAS.

Gli obiettivi del progetto sono:

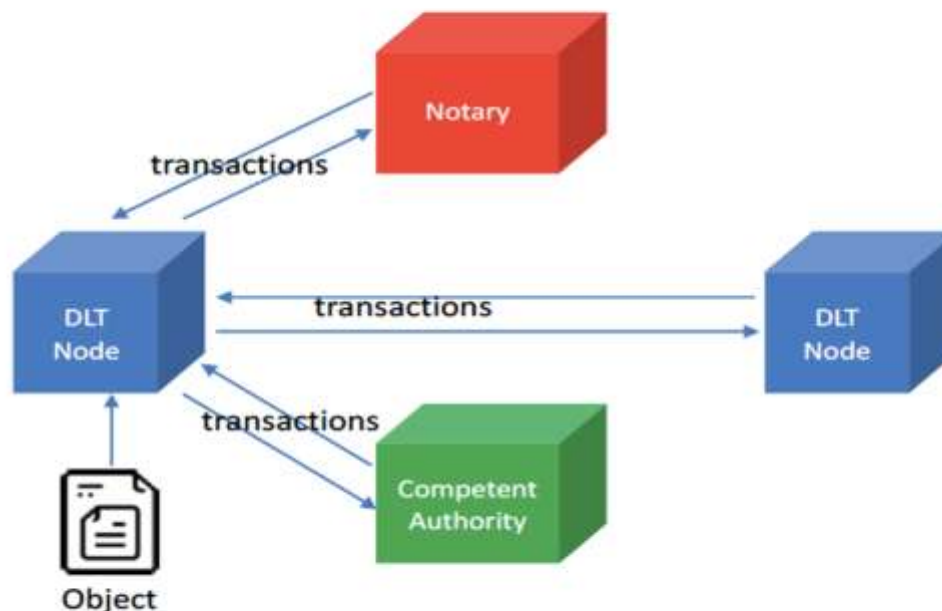
- progettazione, analisi e realizzazione di una architettura destinata ai sistemi di eProcurement coinvolti nella fase di esecuzione delle forniture;
- implementazione di servizi rivolti alle PMI per una completa adozione della EN 16931 "*Semantic data model of the core elements of an electronic invoice*" e dei suoi documenti accessori, con un focus specifico sulla trasformazione digitale in ambito post-award nei contesti B2G e B2B;
- integrazione delle funzionalità di fatturazione elettronica nelle piattaforme di eProcurement esistenti, estendendo i risultati ottenuti nelle precedenti azioni eIGOR (2015-UE-IA-0050) ed EeISI (2017-IT-IA-0150);
- realizzazione di servizi digitali innovativi per la supply chain basati su repository distribuiti e tecnologie DLT, rivolti a diversi settori di mercato ed uno sviluppo verticale nel settore sanitario;
- attività di divulgazione e dissemination per facilitare e promuovere ulteriori adozioni delle fatture EN 16931 in contesti nazionali e transfrontalieri in tutti i settori aziendali sia pubblici che privati.

SCALES implementa dal punto di vista logico il modello Registro distribuito – Repository e il principio Once Only creando un ecosistema dei dati che agevola la relazione tra clienti, fornitori, autorità di controllo abilitando lo sviluppo di servizi a valore aggiunto:



L'approccio decentralizzato dell'architettura di SCALES tiene anche conto che:

- l'**oggetto digitale** viene creato su uno specifico nodo della rete DLT ed è visibile solo al nodo che lo ha creato e a tutti i nodi delle controparti coinvolte in un flusso di lavoro determinato;
- il **Workflow è distribuito** tra diversi nodi, dove ogni nodo partecipa tramite transazione garantita mediante DLT;
- l'unico nodo che ha la **ownership dei dati** è quello sorgente, in cui i dati sono stati caricati. Tutti gli altri nodi, coinvolti nel flusso di lavoro, partecipano ottenendo i dati dal nodo sorgente, elaborandoli e firmando la propria transazione per far progredire il flusso di lavoro;
- il nodo della **Competent Authority** controlla la correttezza dei dati di propria competenza;
- il **nodo Notary** garantisce mediante DLT l'ultimo passo del workflow, per evitare la ripetizione del workflow sulla stessa istanza di dati (**double spending**);
- il sistema è **conforme al GDPR - General Data Protection Regulation (Eu) 2016/679**, come meglio precisato al paragrafo 3.3.



Per lo sviluppo di SCALES sono stati considerati i seguenti assunti:

- la conservazione a norma è un servizio esterno a SCALES, che potrebbe essere fornito da uno o più VAS;
- una volta trascorso il periodo di archiviazione, la fattura elettronica viene eliminata dal repository e sono mantenuti i seguenti metadati:
 - ID unico della fattura,
 - Impronta della fattura,
 - Eventuali dati VAS presenti.

Lo sviluppo di SCALES, considerato lo scopo dello stesso, non ha tenuto conto di una serie di servizi che una piattaforma generalizzata potrebbe implementare di cui si esemplificano alcune possibili caratteristiche:

- l'integrazione nei nodi della conservazione a norma;
- la gestione parametrica del periodo di archiviazione (diverso dalla conservazione a norma) di una fattura elettronica che potrebbe essere modulato su una durata tra alcuni mesi e alcuni anni;
- la determinazione della durata del periodo di archiviazione dovrebbe essere facoltà sia del cedente che del cessionario, che dovrebbero poter decidere questa "policy" secondo

le proprie esigenze (potrebbe quindi essere diverso, a fronte della stessa fattura, per cedente e cessionario);

- l'archiviazione di una fattura elettronica viene effettuata secondo il parametro di archiviazione attivo per ognuna delle controparti e, una volta emessa la fattura elettronica, il periodo di archiviazione per quella fattura non dovrebbe essere cambiato;
- cedente e cessionario dovrebbero poter sempre richiedere la cancellazione immediata di una fattura elettronica, che potrà essere accettata secondo gli accordi in essere e le disposizioni vigenti.

3 UNA PANORAMICA SU BLOCKCHAIN E TECNOLOGIE A REGISTRO DISTRIBUITO (DLT)

Le tecnologie a registro distribuito (Distributed Ledger Technologies, DLT) sono tecnologie che consentono il funzionamento e l'utilizzo di un registro a sola aggiunta, condiviso tra un insieme di nodi e sincronizzato tra essi utilizzando un meccanismo di consenso. Mentre nei Database distribuiti, tutti i nodi hanno una copia del database e possono consultarlo, ma devono passare attraverso un'entità centrale (o più validatori) per modificare i dati, con le tecnologie a registro distribuito, invece, le modifiche al registro sono regolate da algoritmi di consenso. Il registro può essere pertanto letto e modificato in modo indipendente dai singoli nodi.

Specifici algoritmi sono utilizzati per ottenere il consenso tra le diverse versioni del registro, anche se vengono aggiornate in modo indipendente dai membri della rete. Oltre agli algoritmi di consenso, DLT e Blockchain fanno anche un uso diffuso della crittografia per garantire la sicurezza e l'immutabilità del registro condiviso. Blockchain è una tecnologia appartenente alla famiglia delle DLT il cui registro distribuito è strutturato come una sequenza a sola aggiunta di blocchi contenenti transazioni o riferimenti ad esse. Tali blocchi sono confermati, ovvero accettati dai nodi validatori secondo un algoritmo di consenso, e organizzati in una catena mediante collegamenti crittografici.

Inoltre, Blockchain e DLT sono le tecnologie alla base dell'Internet del Valore, che è l'insieme di applicazioni e piattaforme basate su reti di nodi digitali e non legati da relazioni di fiducia che trasferiscono valore attraverso un sistema di algoritmi e regole crittografiche che permette di raggiungere il consenso sulle modifiche ad un registro distribuito tenendo traccia del trasferimento di valore per mezzo di token digitali unici.

3.1 L'EVOLUZIONE DELLA TECNOLOGIA: PASSATO E PRESENTE

Blockchain e DLT stanno attirando sempre più l'attenzione dei media e sono considerati tra le tendenze digitali più interessanti per i prossimi anni. La tecnologia Blockchain è un'invenzione relativamente recente, che risale a poco più di 10 anni fa e che risale alla creazione di Bitcoin e di criptovalute.

In effetti, l'idea innovativa di una moneta virtuale, decentralizzata, p2p, si è affermata come oggi la conosciamo nel 2008, quando è stato pubblicato il libro bianco di Satoshi Nakamoto. Tuttavia, il Bitcoin è stato presto associato al mercato illecito, è stato snobbato da banche e media e considerato un prodotto di nicchia.

Allo stesso tempo, i legislatori hanno sviluppato un approccio conflittuale nei confronti delle criptovalute. In alcuni casi, il Bitcoin era considerato una valuta, mentre in altri era proibito o non raccomandato. Nonostante il quadro scoraggiante, furono create altre piattaforme, basate sugli stessi principi fondanti del Bitcoin, ma che ne hanno esteso il campo di utilizzo, ad esempio Ethereum, Corda, Hyperledger.

Nel 2016 qualcosa è cambiato, all'improvviso la Blockchain era su tutti i media come una delle tecnologie potenzialmente rivoluzionarie e dirompenti del futuro. L'attenzione dei

media, tuttavia, è sempre stata strettamente connessa alle criptovalute, invece che alla tecnologia che sta loro dietro.

La fase di boom del mercato delle criptovalute, caratterizzata da una rapida crescita della capitalizzazione nel 2017, è stata improvvisamente seguita nel 2018 da un forte calo del loro valore: il cosiddetto Cryptowinter.

Non c'è stato però alcun inverno per Blockchain, che, semmai, sta godendo di un'altra primavera, mentre continua a maturare ed evolversi, guadagnando un forte interesse da parte delle aziende di tutto il mondo.

Allora perché questa tecnologia sta attirando così tanta attenzione?

Qual è la vera innovazione introdotta da Blockchain?

È il raggiungimento dell'integrazione efficace di soluzioni tecnologiche consolidate (come la crittografia, funzioni di hash, sistemi distribuiti) per creare un irreprevedibile trasferimento di "valore", indipendente di garanti centrali e potenzialmente anonimo.

Il significato rivoluzionario sta in questo cambiamento di paradigma che può portare alla creazione dell'Internet del Valore: un sistema che permette lo scambio di beni di valore senza intermediari e in modo programmabile utilizzando i cosiddetti smart contract.

Tuttavia, la tecnologia non è ancora del tutto matura, e c'è molta confusione e strumentalizzazione che circonda ciò che può e non può fare.

3.2 I PILASTRI DELL'INTERNET DEL VALORE: ALCUNE DEFINIZIONI E CARATTERISTICHE TECNICHE

Blockchain e DLT sono le tecnologie alla base dell'Internet del Valore, ovvero sistemi che permettono di scambiare valore su Internet con la stessa facilità con cui ci scambiamo le informazioni.

I sistemi DLT si distinguono in base a tre caratteristiche fondamentali: il tipo di rete, il meccanismo di consenso e la struttura del registro.

In base al tipo di rete, i sistemi possono essere permissioned, cioè sistemi in cui gli utenti devono registrarsi e si identificano per essere autorizzati ad accedere; o permissionless, dove chiunque può accedere, senza bisogno di autorizzazione.

Il meccanismo di consenso varia a seconda del tipo di sistema. Nei sistemi permissioned il consenso è più semplice: quando un nodo propone l'aggiunta di una transazione, la sua validità viene controllata e se approvata dalla maggioranza dei nodi può essere aggiunta al registro.

Nei sistemi permissionless, al contrario, gli algoritmi di consenso sono più complessi (basati ad esempio sulla Proof of work o sulla Proof of Stake) per garantire che un individuo malintenzionato non possa creare numerose identità fittizie per influenzare il processo di aggiornamento del registro.

La terza caratteristica dei sistemi DLT è la struttura del registro. Nelle soluzioni Blockchain il registro è strutturato come una catena di blocchi contenenti più transazioni e i blocchi sono collegati l'un l'altro utilizzando la crittografia (come avviene nelle piattaforme Bitcoin o Ethereum). In altre soluzioni, il registro è costituito da Tangle, in cui le transazioni vengono

elaborate in parallelo (ad es. Iota) o ancora altri casi in che il registro è creato da una catena di transazioni (per esempio Ripple).

Inoltre, i sistemi Blockchain permettono agli utenti di effettuare trasferimenti, o più genericamente, transazioni. Queste transazioni possono essere semplici o più complesse, a seconda del livello di programmabilità consentito da la piattaforma. Ad esempio, la piattaforma Ethereum consente la creazione e la gestione di smart contract.

Infine, l'ultima caratteristica dei sistemi Blockchain è che c'è un'attività unica da trasferire, che può essere una moneta cripto o un token.

Le numerose piattaforme che consentono l'Internet del Valore condividono le seguenti caratteristiche:

- Disintermediazione, le piattaforme facilitano la gestione delle transazioni senza intermediario, cioè senza la presenza di entità centrali di fiducia;
- Decentramento, l'informazione viene registrata distribuendola su diversi nodi per garantire sicurezza delle informazioni e resilienza del sistema;
- Immutabilità del registro, una volta che i dati sono stati scritti sul registro non possono più essere modificati senza il consenso della rete;
- Trasparenza del registro, il contenuto del registro è trasparente e visibile a tutti;
- Tracciabilità dei trasferimenti, ogni elemento rappresentato sul registro è rintracciabile a partire dalla sua origine esatta;
- Programmabilità, è possibile programmare che certe azioni siano eseguite quando certi criteri sono soddisfatti. Smart contract, definiti da Nick Szabo come "un insieme di promesse, specificate in forma digitale", compresi i protocolli all'interno dei quali le parti adempiono a queste promesse", sono un fondamentale elemento di alcune piattaforme;
- Digitalizzazione, i dati vengono convertiti in formato digitale.

Nel periodo 2016-2017 sembrava che le soluzioni Blockchain potessero risolvere innumerevoli problemi e aumentare efficienza in molti processi. Diverse aziende, stimolate solo dall'hype dei media, hanno iniziato a sviluppare progetti ed esperimenti senza aver compreso appieno come la tecnologia possa realmente portare valore. Gli sforzi per applicare Blockchain e DLT a casi d'uso non idonei hanno portato scarsi benefici, e la tecnologia in sé è stata incolpata, piuttosto che la sua applicazione concreta.

Per questo motivo, l'Osservatorio Blockchain & Distributed Ledger, attraverso l'analisi di numerosi casi d'uso, ha individuato alcune variabili che devono essere prese in considerazione nella valutazione dell'idoneità di Blockchain e DLT ad un determinato progetto. In particolare, Blockchain e DLT sono particolarmente adatte quando vi è un gran numero di partecipanti che non si fidano l'uno dell'altro (mancanza di fiducia) e necessitano di un sistema condiviso che possa garantire che tutte le copie del registro condiviso siano aggiornate allo stesso modo, in assenza di una terza parte. Inoltre, è importante che questi partecipanti abbiano la necessità di condividere le informazioni, vale a dire che sia utile rendere visibile a un gran numero di soggetti una certa informazione, oppure che debbano trasferire tra loro dei beni, dove si possa garantire che un bene che sia distinguibile e unico e, quindi, non replicabile (unicità del bene). L'asset può essere nativamente digitale o facilmente digitalizzabile (digitalizzazione).

Le Blockchain e DLT possono essere applicate anche alle piattaforme che permettono di programmare che determinate azioni siano eseguite quando sono soddisfatte determinate condizioni tramite l'uso di smart contract (programmabilità variabile).

Infine, Blockchain e DLT possono essere sfruttate appieno e correttamente se i partecipanti considerano come obiettivo principale che le informazioni condivise rimangano immutabili e non possano essere manomesse.

Non è necessario che tutte le condizioni siano pienamente applicabili, né tutte contemporaneamente. Tuttavia, più condizioni sono presenti, tanto più vantaggiosa è l'implementazione che una soluzione basata su Blockchain e DLT può portare.

3.3 I TIPI DI UTILIZZO DI BLOCKCHAIN E MODELLO DLT-REGREP

I progetti che utilizzano Blockchain e DLT possono essere classificati in base al tipo di utilizzo che ne fanno.

La notarizzazione, ad esempio, comprende i progetti che utilizzano il registro distribuito di una Blockchain esistente per registrare la data di un documento e il fatto che non è stato modificato nel tempo (timestamp).

Il meccanismo è garantito dall'utilizzo di funzioni di hash che permettono di creare da un intero documento o database un'impronta (un codice alfanumerico di lunghezza fissa), che può poi essere condiviso sulla Blockchain.

Altri progetti, invece, utilizzano smart contract e sfruttano le reti esistenti e le loro caratteristiche di programmabilità per digitalizzare i processi e creare applicazioni decentralizzate (Dapp).

Ci sono poi progetti che sfruttano le criptovalute già esistenti per consentire lo scambio di valore tra attori che non si conoscono, in mancanza di fiducia. In questi progetti diventa fondamentale la presenza di un asset unico all'interno della piattaforma. Queste tre categorie utilizzano principalmente piattaforme esistenti.

Al contrario, ci sono alcuni progetti che si basano su nuove piattaforme create ad hoc.

È il caso del Distributed Ledger Permissioned e Distributed Ledger Permissionless.

Questi progetti prevedono la creazione di una rete di nodi e di un registro immutabile e distribuito dove le informazioni vengono condivise tra numerosi attori in assenza di fiducia reciproca. Questo modello che non prevede terze parti e nemmeno che vi sia fiducia reciproca tra le controparti viene detto Zero Corner Model (ZCM) per distinguerlo dai classici modelli a 2 lati ovvero con transazioni dirette, possibile solo se tutte le parti hanno fiducia reciproca, a 3 lati ovvero con transazioni tramite un prestatore di servizi che svolge il ruolo di terza parte, possibile se le controparti hanno fiducia nello stesso prestatore, o a 4 lati, ovvero con la presenza di un prestatore di fiducia di ciascuna delle parti e di regola comuni cui tutti i prestatori aderiscono. Il modello a zero lati (ZCM) può essere implementato grazie ad una rete basata su DLT ed il registro distribuito, se la latenza tipica delle soluzioni basate su DLT può essere trascurata, rappresenta l'unica copia condivisa delle informazioni.

Questo permette anche di digitalizzare i processi e di sfruttare la programmabilità degli smart contract, senza però introdurre asset unici per la gestione dei trasferimenti.

Partendo dal presupposto che le stesse informazioni siano disponibili contemporaneamente a ciascun attore che ha il diritto di accedervi, in una rete basata su DLT c'è sempre una latenza, dipendente dalla sua implementazione, necessaria per raggiungere il consenso tra i suoi nodi.

Un registro condiviso per le fatture elettroniche, e la supply chain in generale, non ha necessità di effettuare transazioni in tempo reale, e un'implementazione tipica di DLT è adeguata alla maggior parte dei casi, anche se l'idoneità di una DLT specifica va valutata caso per caso.

Alcuni, o tutti i dati aziendali, possono essere archiviati all'esterno di una DLT utilizzando servizi registro-repository quale, ad esempio, l'OASIS RegRep¹, il cui utilizzo diventa necessario nei casi in cui le proprietà di immutabilità di una DLT sono inadatte, come può essere necessario per il pieno rispetto delle regole sulla privacy (si veda il capitolo 5 per approfondimenti specifici) oppure se vi sono ragioni di riservatezza commerciale rispetto alle informazioni trattate.

Nel caso di SCALES la sua rete DLT implementa un modello DLT-RegRep e le informazioni contenute nel registro condiviso sono collegate ai dati presenti nel registro-repository basato su RegRep per garantirne l'integrità e l'autenticità.

Una DLT dovrebbe quindi:

- fornire un'infrastruttura resiliente per gestire in modo conveniente il volume previsto di documenti e dati;
- fornire una piattaforma a supporto dell'implementazione dei requisiti, in termini di servizi di fatturazione elettronica e di eProcurement, i relativi flussi di lavoro e controllo degli accessi alle informazioni.

Di seguito si indicano alcuni requisiti che sono da considerare quando si progetta una DLT che implementa uno ZCM:

- adozione di un modello basato sulla DLT che adotti il principio Once Only, estendendo il concetto a tutti i diversi attori. Può essere indicato come Provide Data Once Principle (PDOP);
- le parti non inviano documenti, ma li mettono a disposizione dei soggetti interessati e delle autorità fiscali;
- i metadati dei documenti sono archiviati in DLT ed accessibili solo da utenti autorizzati, mentre la DLT stessa ne assicura l'integrità;
- a causa della caratteristica di immutabilità delle DLT, si dovrebbe prestare particolare attenzione per evitare che il dato personale sia presente in chiaro in una DLT, pertanto si dovrebbero prendere in considerazione soluzioni appropriate quali crittografia, anonimizzazione...;
- implementare un migliore controllo e protezione dei dati, scalabilità e prestazioni rispetto all'architettura hub centralizzata. I requisiti di privacy possono essere soddisfatti con il rispetto del principio di accesso "*necessario per sapere*" alle informazioni;
- l'utilizzo di standard comuni è fondamentale come, ad esempio, lo sviluppo della EN 16931:2017 è stato fondamentale per l'interoperabilità, con il possibile riutilizzo, delle informazioni contenute nelle fatture elettroniche.

Nel corso del progetto sono stati prodotti i seguenti documenti:

¹ <http://docs.oasis-open.org/regrep/regrep-core/v4.0/os/regrep-core-overview-v4.0-os.html>

- **Report sulle tecnologie Blockchain e DLT**
Il POLIMI ha condotto una ricerca sulle tecnologie Blockchain e DLT applicabili alla supply chain e al processo di fatturazione elettronica nazionale.
L'analisi ha affrontato l'applicazione di un'architettura basata su DLT alle fasi del ciclo dell'ordine.
- **Disegno della soluzione**
Il documento di Infocert definisce l'architettura generale della rete SCALES, tenendo conto dei risultati dell'analisi dello stato dell'arte sulla tecnologia DLT e i requisiti dell'infrastruttura italiana di eInvoicing (B2B e B2G) e dei sistemi di eProcurement end-to-end.
- **New Service Framework**
Il POLIMI ha condotto un'indagine sull'offerta di servizi a valore aggiunto da parte degli ecosistemi di supply chain esistenti.
Saranno prodotti casi di studio per individuare le criticità dei servizi esistenti e l'appetito delle imprese riguardo nuovi servizi.
- **Studio fattibilità sistemi di eProcurement**
AgID ha coordinato lo studio di fattibilità per l'adozione dell'architettura SCALES da parte dei sistemi di eProcurement nazionali tra cui SDI. Sulla base dei risultati di tale studio è intenzione di AgID aggiornare la Circolare AgID 3/2016 che definisce le regole tecniche aggiuntive per l'interoperabilità dei sistemi di eProcurement ai sensi dell'art.58 comma 10 del Dlgs 50/2016 "Codice dei contratti Pubblici", al fine di agevolare l'adozione di architetture basate su DLT e BC sul modello di SCALES da parte dei sistemi di eProcurement nazionali.
In particolare, lo studio ha analizzato i seguenti aspetti ritenuti critici per l'adozione di tecnologie dei registri distribuiti e blockchain da parte di sistemi di eProcurement e in generale da parte dei sistemi della pubblica amministrazione:
 - 1) Governance
 - 2) Interoperabilità
 - 3) Scalabilità
 - 4) Prestazioni
 - 5) Verificabilità
 - 6) Integrità
 - 7) Sicurezza
 - 8) Privacy (GDPR)
 - 9) Smart contract (legal e non)
 - 10) Gestione dell'identità
- **Componenti software**
Le componenti software dell'architettura SCALES, realizzate da Infocert, saranno pubblicate su Github con licenza EUPL per facilitarne l'adozione e il riutilizzo da parte delle amministrazioni pubbliche e delle imprese del settore privato.
- **Servizi per la filiera Sanitaria**
Il Consorzio DAFNE ha sviluppato una serie di servizi a valore aggiunto (VAS) rivolti ai fornitori del Sistema Sanitario Nazionale sfruttando le potenzialità di SCALES con l'eventuale integrazione verso sistemi di monitoraggio nazionali (SDI, NSO e PCC).

3.4 MODELLO GENERALE DI FUNZIONAMENTO DI SCALES

Per la corretta gestione della privacy, la soluzione adottata è stata quella di tenere separato il nodo della DLT dal layer di persistenza, in modo che l'oggetto digitale (come una fattura) possa essere totalmente o parzialmente cancellabile (ad esempio per eventuali dati sensibili presenti) mantenendo salve le transazioni che hanno coinvolto l'oggetto digitale.

Con l'accordo di servizio viene definito il tempo per il quale l'oggetto rimane memorizzato sul nodo che lo detiene.

La conservazione potrebbe essere effettuata dal nodo in cui l'oggetto digitale viene immesso nel nodo, in modo svincolato rispetto al funzionamento di SCALES.

Il sistema non viene vincolato al rispetto alla "conservazione sostitutiva", essendo quest'ultimo un obbligo autonomo dal Sistema di Interscambio ed esclusivamente in capo al contribuente in base alla vigente normativa fiscale.

In ogni caso il token ha un doppio owner quindi, in caso di cancellazione, entrambi devono essere informati e decidere autonomamente la cancellazione, tenendo presente che entrambi hanno un'autonoma responsabilità rispetto agli obblighi di compliance.

Gli utenti, rispetto alla fattura, sono tre: mittente, destinatario e terza parte.

Le user history possono essere compatibili o no, ed in tal caso occorre fare una scelta:

- 1) quando il mittente chiede di cancellare un documento, il destinatario deve poter essere in grado di continuare ad accedere al documento;
- 2) per la cancellazione automatica essa può avvenire per entrambe le parti dopo un lasso temporale definito dall'accordo di servizio, generalmente coincidente con il termine di conservazione previsto dalla vigente normativa fiscale;
- 3) ognuna delle parti deve essere in grado di accedere ai propri documenti (attivi/passivi) ai fini dell'invio in conservazione;
- 4) nel caso di una terza parte coinvolta in una transazione, il documento può essere verificato mediante l'impronta che è rimasta del documento, permettendo quindi l'accesso ai dati da parte della terza parte anche se mittente e destinatario hanno "cancellato" il documento;
- 5) il documento può essere cancellato definitivamente solo dopo che mittente, destinatario e tutte le eventuali terze parti non hanno più accesso al documento per cancellazione automatica o volontaria;
- 6) eventuali cancellazioni parziali del documento devono essere propagate su tutti i nodi in cui il documento è memorizzato.

4 LA RICERCA CONDOTTA DAL POLITECNICO DI MILANO OSSERVATORIO DIGITALE B2B

4.1 IL RUOLO DELL'OSSERVATORIO DIGITALE B2B

L'Osservatorio Digitale B2b fa parte degli Osservatori dell'Innovazione Digitale della Scuola di Management del Politecnico di Milano, che si propone di sensibilizzare la cultura in tutte le principali aree dell'innovazione digitale attraverso un team di quasi 100 professori, ricercatori e analisti che lavorano in oltre 40 diversi Osservatori su tutti i temi chiave dell'Innovazione Digitale nelle aziende, comprese le PMI, e nel settore pubblico.

La ricerca dell'Osservatorio Digitale B2b è stata condotta come contributo al Progetto SCALES. In particolare, il ruolo dell'Osservatorio Digitale B2b è stato finalizzato a:

- sviluppare una ricerca basata su un'indagine per definire la diffusione e l'interesse delle aziende verso diverse attività, comprendendo al contempo l'impatto della fatturazione elettronica sull'automazione di alcuni di questi servizi;
- definire un quadro di servizio e una roadmap di miglioramento su cui focalizzarsi per investire nella digitalizzazione di queste attività.

4.2 I PRINCIPALI RISULTATI

L'Osservatorio ha realizzato un'indagine CATI, rivolta sia alle PMI italiane che alle grandi imprese, con un campione rappresentativo della popolazione italiana delle imprese, con ponderazione ex ante ed ex post del campione e dei risultati. L'analisi complessiva ha evidenziato alcuni concetti fondamentali:

- Le grandi imprese si concentrano maggiormente sul controllo di gestione, affrontando una complessità più ampia in termini di fornitori e clienti. D'altra parte, le PMI sono più attente alla gestione finanziaria, avendo anche meno necessità e urgenza di gestire la loro catena del valore a monte.
- In generale, la fatturazione elettronica non è stata ancora percepita in modo avanzato all'interno della catena di fornitura: per ora vengono sfruttati solo i benefici delle attività direttamente impattate dall'obbligo, mentre non ci sono investimenti che mirino ad integrarla in processi digitali più completi. Manca quindi la dimensione relazionale ed ecosistemica. Gli investimenti in automazione sono orientati verso attività che tendono ad essere dispendiose in termini di tempo, dove l'azienda ha una visibilità diretta sul tempo dedicato e sul tempo che potrebbe essere risparmiato.

Inoltre, la disponibilità ad investire in attività di automazione già di media intensità dimostra che molte aziende sono ancora in fase di digitalizzazione: dopo gli investimenti iniziali, l'azienda ha percepito i miglioramenti in termini di efficienza ed efficacia legati all'automazione, confermando così ulteriori investimenti futuri per un ulteriore passo evolutivo.

La maggior parte delle aziende, invece, dimostra di non aver ancora implementato una visione a lungo termine: probabilmente non esiste un punto di vista sui processi, quindi è necessario un quadro specifico per capire dove i miglioramenti introdotti con la digitalizzazione avrebbero un impatto.

- Quando si investe in un nuovo sistema per la gestione delle attività, le grandi imprese danno grande importanza alla possibilità di avere una facile integrazione con i sistemi già presenti in azienda.
Questo perché, essendo le grandi imprese, i sistemi software, gestionali e di database sono spesso ben integrati e ben adattati alle esigenze e ai processi dell'azienda stessa, che vuole quindi mantenere lo stesso livello di efficienza con i successivi add-on dei sistemi che verranno introdotti.
Un'altra caratteristica fondamentale per le grandi imprese riguarda la facilitazione del rapporto con i clienti/fornitori nazionali, con l'obiettivo di ottimizzare i flussi all'interno della propria supply chain. In questo contesto, l'introduzione della fatturazione elettronica può certamente avere un impatto positivo.
D'altra parte, per le PMI le preferenze sono più diffuse.
In particolare, va considerato che tra le caratteristiche dei nuovi sistemi, la facilitazione delle relazioni con clienti e fornitori nazionali e quella con clienti e fornitori esteri hanno quasi lo stesso peso.
- Va comunque sottolineato che il settore farmaceutico mostra una maggiore consapevolezza e prontezza nel percepire i miglioramenti legati alla fatturazione elettronica, in particolare in relazione a quelle attività che caratterizzano i rapporti di filiera (vendor e customer rating) e quelle relative all'analisi dei processi interni (process mining).

I dati mostrano quindi che il mercato non è ancora pronto e non è ancora riuscito ad andare oltre l'obbligo, sfruttando la fatturazione elettronica per applicare la digitalizzazione ai nuovi processi aziendali, aumentando l'efficienza e l'efficacia.

L'aspetto chiave è che l'utilizzo della fatturazione elettronica e delle informazioni contenute deve andare oltre l'area amministrativa, in modo che questi dati possano viaggiare più all'interno dell'azienda e contribuire maggiormente alla gestione generale della situazione aziendale all'interno della supply chain, questo per creare un maggiore equilibrio in un ecosistema più ampio.

Maturità non è semplicemente avere processi amministrativi efficienti, ma fare in modo che i dati presenti nella fatturazione elettronica (in modo sintetico) siano rilasciati in tutte le unità di business per dare un maggiore contributo alla conoscenza e al processo decisionale, al fine di meglio inserirli:

- processi di pianificazione;
- logistica;
- produzione;
- marketing....

4.3 IL NUOVO QUADRO DI RIFERIMENTO E LA TABELLA DI MARCIA DELLE ATTIVITÀ

L'Osservatorio ha quindi deciso di aggregare le singole attività in macroaree per meglio apprezzare le differenze tra il gruppo di attività e cercare di dare priorità alle azioni da intraprendere.

Da qui è emerso un quadro complessivo di nuovi servizi che possono essere implementati e la tabella di marcia indicata nella figura seguente.



Le aziende devono necessariamente ottimizzare prima di tutto alcune attività chiave, per ottenere risultati che possano poi essere sfruttati in diversi processi correlati, come indicato in figura.



Queste sono le attività che possono raccogliere i benefici più immediati, a seguito dell'introduzione dell'eOrder e degli obblighi di fatturazione elettronica.

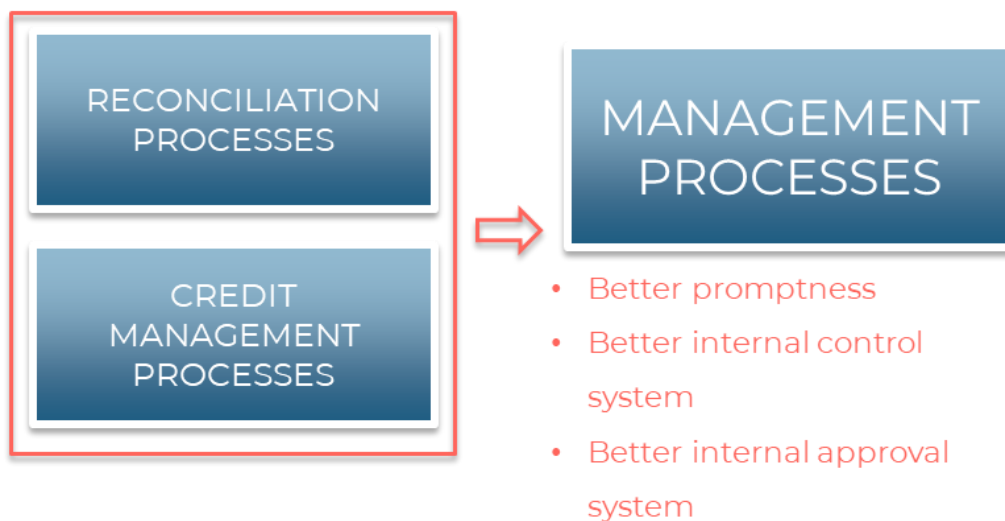
Un'azienda può migliorare questi processi in modo ottimale solo se ha prima perfezionato i processi di riconciliazione, in particolare gli importi ricevuti.

Pertanto, ci concentriamo su questi processi e attività in quanto possono portare a miglioramenti e alla risoluzione di problemi in altri settori.

E poi, quali dovrebbero essere i prossimi passi?

Quali sono i servizi che devono essere ottimizzati?

Sulla base di quanto emerso dalle analisi precedenti, la ricerca ha raccomandato una sequenza delle diverse aree di attività su cui intervenire rappresentata nella figura seguente.



La creazione e lo sviluppo di nuovi servizi può quindi essere ripetuta in modo modulare sui diversi blocchi del framework.

In questo modo, l'azienda può sfruttare l'esperienza già acquisita durante i primi passi nell'ottimizzazione dei processi di riconciliazione e delle attività di gestione del credito.

4.4 UN ULTERIORE PASSO AVANTI: GLI STRUMENTI DI FINANZIAMENTO DELLA SUPPLY CHAIN

Come abbiamo evidenziato, i primi passi riguardano il miglioramento dei processi interni della società, in particolare quelli relativi alle attività finanziarie e gestionali.

Una volta completati questi passi, l'azienda potrà poi concentrare i propri sforzi di ottimizzazione su due diversi percorsi:

- sulle attività legate alla catena del valore interna (acquisti, operazioni, marketing & vendite);
- sulle attività legate alla propria supply chain, in particolare per quanto riguarda gli strumenti di finanziamento della supply chain si veda la figura seguente.



5 REGOLAMENTO (EU) 2016/679 E PRASSI DI RIFERIMENTO UNI/PDR 43:2018

5.1 IL REGOLAMENTO (EU) 2016/679.

Il nuovo quadro normativo europeo della Data Protection ha come scopo la creazione di un sistema coerente e armonizzato a livello comunitario in materia di protezione dei dati personali. È stato presentato dalla Commissione il 25 gennaio 2012 e approvato definitivamente dal Parlamento e dal Consiglio il 27 aprile 2016. I testi definitivi dei provvedimenti sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione europea del 4 maggio 2016 (L 119).

Il quadro normativo attuale della protezione dei dati personali in Europa ed in Italia è rappresentato da:

- General Data Protection Regulation (GDPR) - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) pubblicato sulla G.U. dell'Unione europea del 4 maggio 2016, entrato in vigore il 24 maggio 2016, divenuto efficace il 24 maggio 2018);
- General Data Protection Directive - Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
- Decreto Legislativo 30 maggio 2018, n. 81 Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

Questo quadro di riferimento giuridico serve per:

- creare un quadro normativo unitario, ma in molti ambiti ammette o rinvia a legislazioni derogatorie degli Stati membri,
- contemplare la possibilità o la necessità di specifiche regolamentazioni a livello nazionale in alcune aree lasciate alla competenza delle leggi nazionali degli Stati membri dell'UE,
- mantenere i concetti fondamentali che regolano i ruoli di titolari e responsabili,
- incide e accresce le responsabilità di titolari e responsabili del trattamento,
- incide sul ruolo e sui poteri delle Autorità di controllo nazionali.

Si riportano i più importanti principi di adattamento, integrazione e margini di flessibilità contenuti nei seguenti considerando del Regolamento (EU) 2016/679:

Considerando 8 - Ove il presente regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del regolamento nel proprio diritto nazionale;

Considerando 9 - Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche;

Considerando 10 - Il presente regolamento prevede un margine di manovra degli Stati membri per precisarne le norme, con riguardo al trattamento dei «dati sensibili», per quanto riguarda il trattamento per l'adempimento di un obbligo legale e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

In tal senso, il regolamento non esclude che il diritto degli Stati membri stabilisca con maggiore precisione le condizioni alle quali il trattamento è lecito;

Considerando 11 - Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri.

Il principio dell'Accountability è una novità importante perché introduce il passaggio dalla forma alla sostanza. Infatti, il titolare del trattamento è competente per il rispetto dei principi applicabili al trattamento di dati personali in grado di provarlo («responsabilizzazione»), ed i riferimenti più importanti sono contenuti nei seguenti Considerando:

- 42 Consenso,
- 69 Legittimo interesse del titolare,
- 74 Responsabilizzazione,
- 77 Sicurezza del trattamento,
- 78 Privacy by design,
- 81 Responsabile del trattamento,
- 82 Registro,
- 84 DPIA e
- 85 Data breach.

Le caratteristiche di decentralizzazione, immodificabilità e persistenza delle DLT devono essere valutate e coordinate con le disposizioni in materia di protezione dei dati personali dettate dal Regolamento UE n. 679/2016 – GDPR, finalizzato a disciplinare le ipotesi di trattamento centralizzato degli stessi dati. Come è noto, infatti, tale normativa impone una serie di obblighi a carico del titolare del trattamento, che deve essere di volta in volta individuato. Di conseguenza, l'eventuale trattamento di dati personali svolto tramite il

sistema in esame dovrà rispondere ai principi fondamentali di cui al GDPR (principio di liceità del trattamento, principio della privacy by design e della privacy by default etc.) e dovrà essere fondato sui presupposti di legittimazione del trattamento di cui agli artt. 6 e 9. Un sistema basato su DLT che opera con dati personali rientra infatti nell'ambito di applicazione della normativa sulla protezione dei dati dovendo perciò soddisfare diversi requisiti di legge. Nello specifico, ulteriori profili di criticità possono riguardare:

1. **immodificabilità delle informazioni** inserite in blockchain in caso siano state acquisiti anche dati personali rilevanti a fini privacy; rapporto con diritto all'oblio con possibilità di richiedere la cancellazione dei dati ai sensi dell'art. 17 GDPR: si tratta comunque di un diritto non assoluto in quanto mitigato, ad esempio, dalla presenza di un interesse pubblico oppure al verificarsi delle ipotesi dettate dal comma 3 dell'art. 17 GDPR (esercizio del diritto alla libertà di espressione e di informazione; adempimento di un obbligo giuridico; motivi di interesse pubblico nel settore della sanità pubblica; archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; accertamento, esercizio o difesa di un diritto in sede giudiziaria);
2. **garanzia del diritto di rettifica**, ai sensi dell'art. 16 GDPR, di eventuali dati personali inesatti: da realizzarsi attraverso la richiesta di correzione dati proveniente da tutti i partecipanti alla blockchain e successiva sottoscrizione dei dati così emendati;
3. rispetto del **diritto alla portabilità dei dati** (art. 20 GDPR) attraverso la possibilità di rendere al richiedente i dati personali in un formato elettronico ed interoperabile con sistemi diversi dalla blockchain di origine.

La conoscenza dei principi di protezione dei dati costituisce ad ogni modo la base per *“attuare misure tecniche e organizzative adeguate”*: nel dettaglio, l'art. 25 GDPR (art. 25 GDPR) dispone infatti circa il principio **privacy by Design e by Default** e cioè *“la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita”*. Si tratta di un obbligo generale secondo cui: *“tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso”* il Titolare del trattamento dei dati *“mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati”*.

Alla luce dei principi della **Privacy by Design e by Default**, dunque, il titolare del trattamento deve assicurarsi di mettere in atto *“misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento”*. In tal senso *“tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. Ciò significa che tali “misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica”*. In questo ambito, è previsto infine un meccanismo di certificazione che *“può essere utilizzato come elemento per dimostrare la conformità ai requisiti”* sopra citati.

Principi di protezione dei dati e rischi connessi

La realizzazione di sistema DLT o Blockchain non può quindi non tenere conto, quando contenga dati personali, dei principi della privacy by design in una fase iniziale. I principi da considerare, individuati all'art. 5 GDPR, sono:

- (i) limitazione della finalità: i dati raccolti ed elaborati devono soddisfare uno scopo predefinito e quindi avere delle finalità determinate, esplicite e legittime, per essere successivamente trattati in un modo che non sia incompatibile con tali finalità. Finalità *ad hoc* distinte da quelle inizialmente stabilite per l'ulteriore trattamento dei dati personali sono contrarie a questo principio fondamentale della protezione dei dati. Di conseguenza, il riutilizzo dei dati personali per uno scopo non previsto inizialmente è contrario al principio della limitazione della finalità.

Se il principio della limitazione delle finalità non venisse rispettato, i dati potrebbero essere trattati in modo contrario alle informazioni rese nell'informativa che l'interessato ha ricevuto al momento della condivisione;

- (ii) esattezza: il principio impone ai responsabili del trattamento di assicurarsi che i dati personali siano “*esatti e, se necessario, aggiornati*”. In caso contrario, devono essere “*cancellati o rettificati*” tempestivamente. In altri termini, se i dati sono inesatti devono essere rettificati. Nei sistemi basati su DLT, la possibilità di cancellare o rettificare i dati inesatti comporta problemi specifici dovuti alla funzionalità distribuita e alla proprietà di immutabilità. Tuttavia, se l'unico scopo dell'applicazione è quello di documentare il verificarsi di un fatto in un determinato momento (attraverso la combinazione di un dato con una marca temporale, non tentando quindi di descrivere lo stato attuale delle cose) non pare vi siano criticità in relazione al principio dell'esattezza;
- (iii) minimizzazione dei dati e limitazione della conservazione: la minimizzazione consiste nella raccolta e nel trattamento di un numero limitato di dati; tali dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. I dati possono essere minimizzati dalla fonte (cioè al momento della loro raccolta) o ridotti allo stretto necessario se importati da una fonte esistente. Le autorità di controllo potranno verificare l'adozione di misure tecniche e organizzative proporzionate al rischio per la persona interessata. La mancata minimizzazione dei dati aumenta il rischio per i diritti e le libertà della persona interessata. Si raccomanda pertanto che un sistema basato su DLT sia progettato in modo da considerare il requisito della minimizzazione dei dati nella fase iniziale di progettazione, in ossequio al principio di *privacy by design*;
- (iv) riservatezza e integrità: secondo il considerando 39, del Regolamento GDPR i dati personali GDPR devono “*essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento*”. La garanzia di questo principio richiede sia la conoscenza di quali dati non devono essere divulgati a terzi, sia l'applicazione di adeguate misure tecniche e organizzative per salvaguardare i dati dalla divulgazione. Nei sistemi basati su DLT potenzialmente tutti o molti nodi potrebbero essere a conoscenza dei dati personali. È quindi necessario trovare un equilibrio tra la visibilità di alcuni dati per mantenere il sistema funzionale e distribuito e l'applicazione di misure tecniche per salvaguardare i dati personali da accessi non autorizzati;

- (v) *trasparenza*: si tratta di un principio fondamentale della protezione dei dati. Il GDPR richiede che il trattamento dei dati venga effettuato in modo equo e trasparente. L'obbligo di informare l'interessato è il corollario dell'obbligo di trasparenza del trattamento dei suoi dati. Gli interessati devono essere informati in modo completo degli aspetti rilevanti del trattamento (ad es. da chi sono raccolti i dati per quali scopi, per quanto tempo i dati sono conservati, chi potrebbe eventualmente ricevere tali dati, quali diritti sono loro applicabili, come far valere tali diritti etc.). Il rischio che potrebbe conseguire al mancato rispetto principio di trasparenza è quello di non comunicare lo scopo e la portata dei dati trattati sulla rete DLT. Si dovrebbe quindi cercare di chiarire questi aspetti con contenuti informativi che siano accessibili e presentati al pubblico a cui la soluzione è destinata.

Ulteriori requisiti

Tra gli ulteriori requisiti previsti dal Regolamento GDPR che dovrebbero caratterizzare ogni trattamento di dati personali vi sono:

- 1) ***diritto all'oblio*** (art. 17 GDPR): il diritto alla cancellazione dei dati personali senza ingiustificato ritardo è tecnicamente possibile su un unico computer da un punto di vista tecnico. L'attuazione di questo diritto in un sistema basato su DLT è relativamente più difficile perché la cancellazione sul computer di un singolo nodo non comporta la cancellazione in tutta la rete. Sebbene siano state proposte alcune misure tecniche per cancellare specifici contenuti delle transazioni da un DLT, ciò dipende fortemente dall'esistenza di un meccanismo di *governance* applicabile che consenta la cancellazione "senza ingiustificato ritardo" su richiesta di una persona interessata;
- 2) ***immutabilità delle registrazioni***: l'art. 17(3) GDPR disciplina le esenzioni dall'obbligo di cancellare i dati su richiesta dell'interessato. Se un sistema basato su DLT è in grado di rispettare una delle esenzioni previste, la caratteristica di immutabilità di una rete DLT può essere giustificata e ammessa;
- 3) ***diritto di rettifica*** (art. 16 GDPR): quando i dati non sono corretti, l'interessato ha il diritto di chiederne la rettifica. Nei sistemi basati su DLT non è del tutto chiaro se il requisito richiesto è soddisfatto con un'ulteriore immissione di dati, a correzione delle informazioni errate senza la completa cancellazione dei precedenti dati. Anche se le informazioni o le transazioni possono essere invalidate con i nuovi blocchi aggiunti, chiunque può visualizzare dati errati. Anche se questa soluzione tecnica fosse sufficiente, la sua attuazione rappresenterebbe comunque un ostacolo significativo al rispetto di tale requisito;
- 4) ***diritto alla portabilità dei dati*** (art. 20 GDPR): il diritto alla portabilità dei dati consente all'interessato di richiedere ad un titolare del trattamento, in formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti. Poiché la portabilità dei dati è in primo luogo la risposta ad un problema che si presenta nei sistemi in formato chiuso, essa può essere risolta più facilmente nei sistemi basati su DLT se vengono applicati standard comuni di interoperabilità;
- 5) ***informazioni da fornire agli interessati*** (art. 13 e art. 14 GDPR): i titolari del trattamento sono tenuti ad informare gli interessati sul trattamento dei dati personali che li riguardano. Nei sistemi basati su DLT, ciò può presentare degli aspetti di incertezza, poiché il ruolo del titolare del trattamento è difficile da individuare;

- 6) **processo decisionale automatizzato (art. 22 GDPR)**: l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. L'obiettivo dell'art. 22 GDPR è proprio quello di stabilire elevate garanzie per i processi decisionali completamente automatizzati che comportano conseguenze legali per la persona interessata. Anche se le applicazioni che si basano su reti DLT spesso implementano processi altamente automatizzati (ad es. *smart contract*), dipende fortemente dal caso d'uso individuale se questa funzionalità costituisce una decisione che rientra nell'ambito di applicazione dell'art. 22 GDPR. Il responsabile del trattamento attua misure adeguate per salvaguardare i diritti e le libertà dell'interessato e i suoi legittimi interessi, almeno il diritto di ottenere l'intervento umano;
- 7) **minimizzazione dei dati (articolo 5, paragrafo 1, lettera c) GDPR)**: in un sistema basato su DLT una delle possibili modalità tramite cui favorire il rispetto del principio di minimizzazione dei dati può consistere nella pseudonimizzazione dei dati con l'uso di funzioni *hash*. Nel caso di una rete DLT che garantisce immutabilità dei dati, la minimizzazione degli stessi deve essere presa in considerazione già durante il processo di sviluppo, poiché la successiva modifica è tecnicamente difficile da realizzare, se non impossibile, per le proprie caratteristiche intrinseche delle DLT;
- 8) **diritto di accesso da parte dell'interessato (art. 15 GDPR)**: l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali. Rispetto ad un sistema centralizzato, potrebbe essere ancora più facile per l'interessato accedere alle informazioni necessarie in un sistema basato su DLT trasparente. Tuttavia, l'applicazione di questo diritto in una rete distribuita potrebbe presentare delle difficoltà tecniche che devono essere affrontate con metodi di *governance*.

Il progetto SCALES, per consentire un'implementazione flessibile e rispettosa dei requisiti privacy ha adottato il modello DLT-RegRep, che consente da un lato di sfruttare le garanzie di immutabilità proprie di una rete DLT a garanzia dell'integrità delle transazioni e delle informazioni, dall'altro consente tramite un servizio registro-repository (RegRep) di poter ottemperare ai requisiti normativi mantenendo il controllo sulle informazioni, come meglio descritto nel paragrafo 3.3.

Quanto precede ha visto anche l'emanazione di norme applicabili per le **certificazioni** che si possono suddividere in:

CERTIFICAZIONI REGOLAMENTATE,

che si basano su Leggi, Regolamenti, Direttive.

La certificazione si fonda sul rispetto obbligatorio della normativa prevista da Leggi dello Stato e dai Regolamenti o Direttive dell'Unione Europea.

CERTIFICAZIONI VOLONTARIE

che sono norme tecniche di derivazione privatistica.

La scelta di aderire alla certificazione è totalmente volontaria, non essendo stabilita da norme di legge.

Le certificazioni pertanto si basano su documenti di riferimento o di normazione tecnica. Alcune certificazioni sono basate sugli schemi conformi alla norma di accreditamento ISO/IEC 17065 come:

- **UNI/PdR 43.2:2018** – Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento (EU) 2016/679 (GDPR) – Requisiti per la protezione e valutazione di conformità dei dati personali in ambito ICT;
- Lo schema di certificazione proprietario **ISDP©10003:2015** sviluppato da INVEO, prima dell'entrata in vigore del Regolamento (EU) 2016/679.

L'ISO ha emesso la norma **ISO/IEC 27701:2019** Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines che può essere utilizzata per la certificazione del sistema di gestione di ogni soggetto che tratta dati personali.

Con in corso attività nell'ambito **CEN/CENELEC/JTC 13/WG 5** per scrivere una norma basata sulla ISO/IEC 27701 che ne consenta l'utilizzo nell'ambito di schemi di certificazione basati sulla norma **ISO/IEC 17065** come richiesto dall'articolo 43 del GDPR per le certificazioni emesse ai sensi dell'articolo 42.

La certificazione dei profili professionali in ambito protezione dei dati è possibile ai sensi della Legge 4/2013 secondo la Norma **UNI 11697**, che definisce le figure di:

- Responsabile della protezione dei dati,
- Manager Privacy,
- Verificatore Privacy,
- Specialist Privacy.

Si ritiene opportuno richiamare, a proposito delle certificazioni in ambito privacy, quanto scritto nel comunicato congiunto del Garante Privacy e ACCREDIA²: *“al fine di indirizzare correttamente le attività svolte dai soggetti a vario titolo interessati in questo ambito – che al momento le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le parti interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi “conformi agli artt. 42 e 43 del regolamento 2016/679”, poiché devono ancora essere determinati i “requisiti aggiuntivi” ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione.”*

5.2 PRASSI DI RIFERIMENTO UNI/PDR 43:2018

La Prassi di Riferimento UNI/PdR 43:2018 “Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR)” è stata elaborata dal Tavolo "Processi di gestione privacy in ambito digitale", sotto il coordinamento di UNINFO, che lavora nell'ambito delle tecnologie informatiche e delle loro applicazioni.

La prassi di riferimento si compone di due sezioni:

- **UNI/PdR 43.1** "Gestione e monitoraggio dei dati personali in ambito ICT";
- **UNI/PdR 43.2** "Requisiti per la protezione e valutazione di conformità dei dati personali in ambito ICT.

La sezione 1 fornisce le linee guida per la definizione e attuazione dei processi riguardanti il trattamento dei dati personali mediante strumenti elettronici (ICT), secondo il Regolamento Europeo 679/2016 e la normativa vigente.

² <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6621723>

La sezione 2 fornisce un adeguato insieme di requisiti che permette alle organizzazioni, in particolare le PMI, di essere conformi a quanto previsto dal quadro normativo europeo e nazionale in modo efficace, potendo dimostrare tale conformità ed efficacia anche attraverso un percorso di certificazione.

Solo la UNI/PdR 43.2 può essere usata per attività di certificazione.

Cosa vuol dire certificarsi?

Significa avere una pianificazione conforme ed una corretta gestione in materia di:

- Risk Management per i dati personali,
- Piano di implementazione per la «protezione dei Dati Personali»,
- PIA - Privacy Impact Assessment,
- Il Consenso dell'interessato,
- Strumenti operativi innovativi,
- La protezione fin dalla progettazione (by design e by default!),
- I registri dei trattamenti,
- Aspetti economici e sinergie,
- Data Breach,
- Ruolo del Data Protection Officer.

6 ALLEGATI

6.1 **TERMINI & DEFINIZIONI:**

- ITU: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf>
- ISO: <https://www.iso.org/obp/ui#home>
- UNCEFACT:
https://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain_TechApplication.pdf, Annex II.

6.2 **FONTI DA TENERE IN CONSIDERAZIONE**

- DI 135/2018 Art. 8 ter <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2018-12-14;135!vig=>
- Blockchain - Consultazione pubblica “Proposte per la Strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain”
<https://www.mise.gov.it/index.php/it/consultazione-blockchain#documento>
- Linee guida modello Interoperabilità <https://docs.italia.it/italia/piano-triennale-ict/lg-modellointeroperabilita-docs/it/bozza/doc/doc02cap07.html>
- Regolamento eIDAS <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32014R0910&from=ES#d1e2942-73-1->
- REGULATION (EU) 2018/1724 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 2 October 2018 “establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012”. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L.2018.295.01.0001.01.ENG>
- Circolare Accredia su eDelivery eIDAS
<https://www.accredia.it/app/uploads/2020/03/CircolaretecnicaDC05-2020.pdf>
- Blockchain and the General Data Protection Regulation
<https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRSSTU%282019%29634445>
- Study on blockchains. Legal, governance and interoperability aspects – Study
<https://op.europa.eu/en/publication-detail/-/publication/c7d71ce2-5782-11ea-8b81-01aa75ed71a1/language-it>
- JRC Report “Blockchain Now And Tomorrow - Assessing Multidimensional Impacts of Distributed Ledger Technologies”
<https://ec.europa.eu/jrc/en/facts4eufuture/blockchain-now-and-tomorrow>
- EU Blockchain Observatory and Forum reports
<https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRSSTU%282019%29634445>
- PEPPOL Continuous Transaction Controls Project, Tax clearance and reporting models. <https://peppol.eu/wp-content/uploads/2019/09/20191105-Hoddevik-on-Peppol-André-Hoddevik.pdf>
- PEPPOL Presentazione CTC project Reference Group 20 maggio 2020.

6.3 **NORME TECNICHE E RACCOMANDAZIONI INTERNAZIONALI**

ISO/TC 307 Blockchain and distributed ledger technologies

(<https://www.iso.org/committee/6266604.html>)

- ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary
 - ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations
 - ISO/TR 23455:2019 Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
 - ISO/CD TR 23245.2 Blockchain and distributed ledger technologies — Security risks, threats and vulnerabilities
 - ISO/CD 23257.3 Blockchain and distributed ledger technologies — Reference architecture
 - ISO/CD TR 23576 Blockchain and distributed ledger technologies — Security management of digital asset custodians
- DIN SPEC 4997 (PAS) Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology
<https://www.din.de/en/innovation-and-research/din-spec-en/business-plans/wdc-beuth:din21:303231492>
- PAS 333:2020 PAS 333:2019, Smart Legal Contracts – Specification
<https://standardsdevelopment.bsigroup.com/projects/2018-03267#/section>
- ESI Policy and security requirements
- ETSI EN 319 401
<https://www.etsi.org/deliver/etsien/319400319499/319401/02.02.0020/en319401v020200a.pdf>
 - ETSI EN 319 521
<https://www.etsi.org/deliver/etsien/319500319599/319521/01.00.0020/en319521v010000a.pdf>
- UNCEFACT
- Transport, Trade Logistics and Trade Facilitation, Seventh session: Trade facilitation and transit in support of the 2030 Agenda for Sustainable Development
 - https://unctad.org/system/files/non-official-document/cimem7p16_Lance%20Thompson_en.pdf

6.4 LA DIRETTIVA 2014/55/UE SULLA FATTURAZIONE ELETTRONICA NEGLI APPALTI PUBBLICI

La fatturazione elettronica costituisce il punto di snodo del processo di digitalizzazione dei processi di approvvigionamento, di pagamento della fornitura, di assolvimento del pagamento delle imposte, della contabilità e di audit da realizzare mediante l'implementazione anche degli standard europei relativi all'eProcurement end-to-end che sono in corso di definizione presso il CEN/TC 434 e CEN/TC 440, che rappresentano un elemento chiave per contribuire agli obiettivi di crescita sostenibile indicati dalla Strategia di EU 2020 con la "Comunicazione della Commissione europea (2013) 453 Appalti elettronici end-to-end per modernizzare la pubblica amministrazione".



L'eProcurement end-to-end non riguarda l'implementazione di un progetto IT che replicherebbe solo i processi basati su carta; è un'opportunità per ripensare radicalmente il modo in cui è organizzata la pubblica amministrazione, e tale ripensamento lo si sta affrontando anche con tecnologie di ultimissima generazione.

L'Italia ritiene fondamentale raggiungere la conformità sia con la fattura elettronica europea sia con il processo di gestione digitale degli acquisti della PA per ridurre i costi e creare nuove efficienze e valore. La conformità da sola non richiede un significativo stravolgimento, infatti esisteva già il formato Fattura PA, ma il potenziale di risparmio è insito nell'aggiunta di nuovi livelli automazione della gestione della fattura elettronica che permettono anche di migliorare sia il contrasto all'evasione sia la lotta alle frodi in materia di IVA. La Direttiva richiedeva la definizione di una norma europea che definisse un modello semantico comune sulla fatturazione elettronica e ulteriori documenti di normazione per migliorare l'interoperabilità a livello di sintassi.

L'articolo 1 della Direttiva 2014/55 specifica che essa si applica alle fatture elettroniche emesse a seguito dell'esecuzione di contratti a cui si applicano:

- Direttiva 2009/81/CE relativa al coordinamento delle procedure di aggiudicazione di determinati appalti di lavori, contratti di fornitura e appalti di servizi da parte di amministrazioni aggiudicatrici o enti nei settori della difesa e della sicurezza,
- Direttiva 2014/23/UE relativa alla aggiudicazione di contratti di concessione,
- Direttiva 2014/24/UE sugli appalti pubblici o Direttiva 2014/25/UE sugli appalti enti che operano nel settore idrico, dell'energia, dei trasporti e dei servizi postali.

La Direttiva stabilisce che l'obbligo di ricevere fatture elettroniche *"non si applica alle fatture elettroniche emesse a seguito dell'esecuzione di contratti che rientrano nell'ambito di applicazione della direttiva 2009/81/CE, qualora l'aggiudicazione e l'esecuzione del contratto siano dichiarate segrete o debbano essere accompagnate da speciali misure di sicurezza secondo le disposizioni legislative, regolamentari o amministrative vigenti in uno Stato membro e a condizione che lo Stato membro stesso abbia determinato che gli interessi essenziali in questione non possono essere garantiti da misure meno restrittive"*.

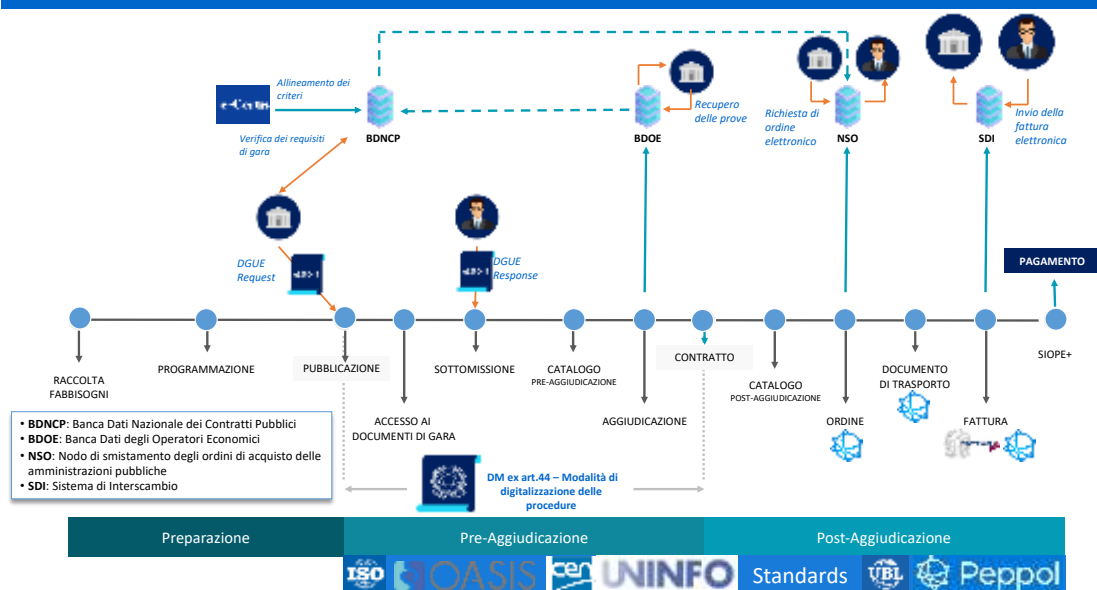
Esiste un obbligo di ricevere ed elaborare, quindi il fornitore avrà la possibilità di inviare fatture elettroniche al destinatario e, in tal caso, si dovrà garantire che la fattura sia ricevuta ed elaborata, con conseguente pagamento o altra risposta possibile dal destinatario all'acquirente (integrazione informazioni, rifiuto, ...). La Direttiva non impone ai fornitori di inviare fatture elettroniche, ma gli Stati membri o i singoli destinatari possono imporre tali requisiti come parte dell'adozione della Direttiva.

La ricezione delle fatture elettroniche richiede l'adozione di una o più soluzioni a livello di trasmissione. Né la Direttiva né la norma sulla fattura elettronica specificano come devono essere trasmesse le fatture elettroniche, ma lo standard fornisce linee guida sull'interoperabilità delle fatture elettroniche a livello di trasmissione, individuando opzioni e formulando raccomandazioni. Le opzioni di trasmissione accettate possono essere individuate negli Stati membri come parte del recepimento nazionale della Direttiva.

La norma definisce la semantica e la sintassi (formato) della fattura elettronica europea, e non dispone alcuna prescrizione in merito alla l'infrastruttura di trasporto utilizzata.

La Direttiva non specifica come devono essere elaborate le fatture. La norma EN 16931-1:2017 specifica quali sono i processi aziendali supportati dallo standard, il che significa che un destinatario pienamente conforme alla EN 16931-1:2017 riceverà ed elaborerà tutte le fatture che richiedono uno dei processi supportati. Lo standard non specifica come devono essere elaborate le fatture, il che lascia al destinatario decidere in merito al livello di automazione che desidera adottare.

La digitalizzazione degli acquisti pubblici



Il tutto per transitare l'Italia verso il Mercato Unico Digitale attraverso queste azioni:

- **eProcurement & eInvoicing:** con il recepimento delle Direttive 2014/24/EU e 2014/55/EU, si è permesso alle Pubbliche Amministrazioni di migliorare l'efficienza amministrativa. Mentre per le Imprese, con l'accesso al Mercato unico, si è già assistito ad una riduzione degli oneri amministrativi, all'automazione dei flussi documentali specie in ottica transnazionale (EN 16931);
- **Sportello Unico Digitale:** con l'emanazione del Regolamento UE 2018/1724 il Single Digital Gateway (Once Only) faciliterà l'accesso alle informazioni, alle procedure amministrative e ai servizi di assistenza necessari a cittadini e imprese per essere attivi nel Mercato Unico;
- **Libera circolazione dei dati non personali:** l'introduzione del Regolamento UE 2018/1807 permette di migliorare la mobilità transfrontaliera dei dati non personali nel mercato unico, con l'obiettivo di garantire l'accesso ai dati da parte delle autorità nazionali competenti, agevolare il porting dei dati tra i fornitori di servizi di memorizzazione e trattamento;
- **Mercato Unico dei Capitali:** con la Comunicazione COM/2020/66 Obiettivi di promuovere: un'economia agile basata sui dati; un ecosistema che crei nuovi prodotti e servizi basati sui dati; la condivisione di dati tra imprese; incremento della pubblicazione dei dati pubblici.

In particolare, con la Comunicazione COM (2020) 66 del 19 febbraio 2020 la Commissione faciliterà l'elaborazione di standard e requisiti comuni europei per i servizi di elaborazione dei dati relativi agli appalti pubblici.

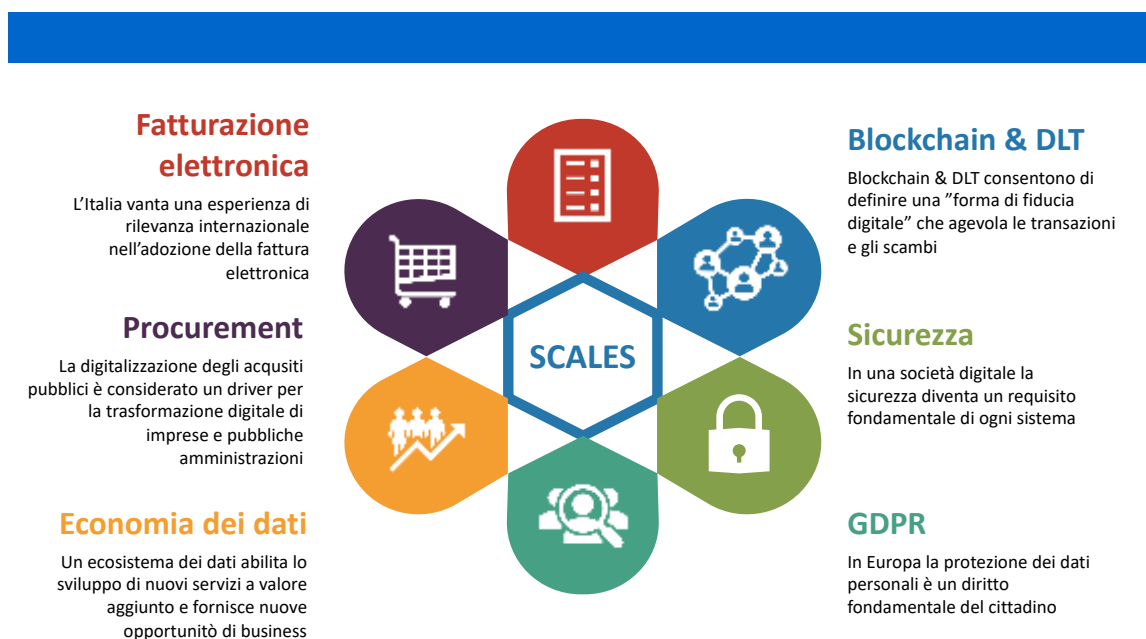
Ciò consentirà al settore pubblico dell'UE a livello europeo, nazionale, regionale e locale di divenire anch'esso un motore per nuove capacità di elaborazione dati dell'UE, invece di essere un semplice beneficiario di tali infrastrutture europee.

I dati sugli appalti pubblici sono essenziali per aumentare la trasparenza e la responsabilità nella spesa pubblica, lottare contro la corruzione e migliorare la qualità della spesa.

Attualmente negli Stati membri tali dati sono distribuiti su vari sistemi e sono resi disponibili in diversi formati, il che non li rende facilmente utilizzabili in tempo reale a fini strategici. In molti casi la loro qualità deve essere migliorata.

La Commissione elaborerà un'iniziativa per i dati sugli appalti pubblici che contempli sia la dimensione UE (set di dati dell'UE, come TED) sia quelle nazionali (4° trimestre 2020) e l'iniziativa sarà accompagnata da un quadro sulla governance dei dati sugli appalti (2° trimestre 2021).

In questo contesto il progetto SCALES si posiziona come indicato nella figura seguente.



L'automazione dei processi di business e delle comunicazioni fiscali si è evoluta in modo indipendente. Nei casi peggiori tax reporting, financial supply chain e physical supply chain costituiscono silos completamente separati. Nei casi virtuosi le imprese hanno integrato la supply chain finanziaria e fisica e per fare questo buyer e seller arrivano a scambiarsi fino a 160 messaggi.

A livello globale si sta assistendo ad un aumento del numero delle comunicazioni richieste dalle autorità fiscali e i flussi informativi verso le autorità si sovrappongono e sono eseguiti in parallelo con i flussi informativi dei processi di business.

La tendenza è quindi che le tre aree vadano a coincidere creando un unico ecosistema dei dati.

- **Tax reporting** con Autorità fiscali, imprese con gli obiettivi del controllo dell'evasione, attraverso la raccolta ed il controllo dei dati fiscali;
- **Financial supply chain** per le imprese e le istituzioni finanziarie, per andare a finanziare il capitale circolante;
- **Physical supply chain** per le imprese;
- Obiettivi: tenere sotto controllo e ottimizzare la catena di distribuzione/approvvigionamento.

6.5 LO STANDARD EUROPEO SULLA FATTURA ELETTRONICA EN 16931:2017

La fattura elettronica deve essere conforme allo standard europeo sulla fatturazione elettronica rappresentato dalla [EN 16931-1:2017](#).

Le stazioni appaltanti devono essere in grado di ricevere ed elaborare fatture elettroniche utilizzando una qualsiasi delle due [sintassi specificate](#) nell'elenco di sintassi (EN 16931-2:2017) conformi alla norma EN 16931-1:2017.

La norma europea in materia di fatturazione elettronica è stata formalmente pubblicata da parte del Comitato Europeo di Normazione (CEN) in 6 parti insieme con le specifiche tecniche e i rapporti tecnici a supporto tra giugno e ottobre 2017.

Lo standard sulla fattura elettronica pubblicato dal CEN rappresenta un modello di dati semantico degli elementi essenziali della fattura elettronica: non è riconducibile ad uno specifico formato, ma è un modello che permette di descrivere il contenuto essenziale di una fattura, il core semantic model, assicurando la rispondenza del modello dati alla direttiva 2006/112 CE (Direttiva IVA) e le norme in materia di IVA dei singoli Stati membri nonché la normativa primaria degli stessi.

Insieme con il modello di dati semantico è stata pubblicata la specifica tecnica TS 16931-2:2017 che contiene la lista delle sintassi.

Il requisito di supportare molteplici sintassi ha sollevato molte questioni nel CEN/TC 434, di tipo operativo e di costo, in relazione agli interessi, investimenti, di specifici Stati membri e comunità.

La richiesta di normazione della Commissione conteneva solo requisiti qualitativi, e si è discusso lungamente se:

- limitare a 1 o 2 sintassi la lista oppure adottare un approccio più ampio,
- limitare la tecnologia di base a XML o includere EDIFACT.

Dopo un'analisi circostanziata, il comitato CEN/TC 434 ha stabilito di inserire nella specifica tecnica TS 16931-2 le seguenti sintassi:

- ISO/IEC 19845:2015 / OASIS Universal business language (UBL v2.1)
- UN/CEFACT Cross Industry Invoice XML (nella sotto-parte 4).

Il supporto ufficiale di UN/EDIFACT è stato ritenuto essenziale in considerazione del suo uso largo utilizzo nel settore privato, ma si evidenzia che è facoltativo.

La serie EN 16931 completa è composta come indicato nella tabella seguente.

Nome	Numero	Tipo
Modello di dati semantico degli elementi essenziali di una fattura elettronica	EN 16931-1: 2017	Norma europea
Elenco delle sintassi conformi alla norma EN 16931-1	CEN/TS 16931-2: 2017	Specifica tecnica
Metodologia per le mappature sintattiche degli elementi essenziali di una fattura elettronica	CEN/TS 16931-3-1: 2017	Specifica tecnica
Mappature sintattiche per fatture e note di credito ISO/IEC 19845 (UBL 2.1)	CEN/TS 16931-3-2: 2017	Specifica tecnica
Mappature sintattiche per UN/CEFACT XML Cross	CEN/TS 16931-3-3: 2017	Specifica

Industry Invoice D16B		tecnica
Mappature sintattiche per UN/EDIFACT INVOIC D16B	<u>CEN/TS 16931-3-4: 2017</u>	Specifica tecnica
Linee guida sull'interoperabilità delle fatture elettroniche a livello di trasmissione.	<u>CEN/TR 16931-4: 2017</u>	Rapporto tecnico
Linee guida sull'utilizzo di estensioni settoriali o nazionali in combinato disposto con EN 16931-1, metodologia da applicare nell'ambiente reale.	<u>CEN/TR 16931-5: 2017</u>	Rapporto tecnico
Risultato della verifica della norma EN 16931-1 rispetto al suo utilizzo pratico da parte dell'utilizzatore finale	<u>CEN/TR 16931-6: 2017</u>	Rapporto tecnico

6.6 I SERVIZI OFFERTI DALL'AGENZIA DELLE ENTRATE PER EMISSIONE, ARCHIVIAZIONE FATTURE ELETTRONICHE

L'obbligo della conservazione delle fatture elettroniche attive e passive disciplinato dal Decreto Ministeriale del 17 giugno 2014 *“Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione su diversi tipi di supporto”*, di cui all'articolo 21, comma 5, del Decreto Legislativo n. 82/2005, si aggiunge agli altri adempimenti obbligatori previsti per i soggetti passivi IVA dalla normativa civilistica e fiscale in relazione alla conservazione.

Con il Provvedimento 89757 del 30 aprile 2018 l'Agenzia delle Entrate ha comunicato che tutti i soggetti passivi IVA residenti, stabiliti o identificati in Italia possono aderire, mediante servizio online, ad apposito accordo di servizio e usufruire gratuitamente del servizio di conservazione a norma di tutte le fatture elettroniche emesse o ricevute dall'operatore attraverso il Sistema di Interscambio.

Con il successivo Provvedimento 524526 del 21 dicembre 2018 l'Agenzia delle Entrate è intervenuta per risolvere le criticità segnalate dall'Autorità Garante per la tutela dei dati personali, recependo le soluzioni emerse nei lavori del tavolo tecnico congiunto Ministero Finanze, Agenzia delle Entrate e Autorità Garante per i dati personali. Il documento ha modificato i provvedimenti precedentemente emessi dal Direttore dell'Agenzia delle Entrate, introducendo novità anche sul sistema di conservazione. I contribuenti avevano a disposizione 60 giorni, a partire dal 3 maggio, per decidere se aderire al sistema di conservazione dell'Agenzia delle Entrate, collegarsi al portale Fatture e Corrispettivi e confermare la volontà di attivare il servizio che permette la conservazione delle fatture elettroniche. Per chi aderisce c'è sempre la possibilità di revoca, da effettuare tramite il portale. L'Agenzia delle Entrate, al termine del periodo transitorio, cancellerà le fatture elettroniche memorizzate nei primi sei mesi di vita del documento nella sua versione 2.0.

Con il Provvedimento n.311557/2020 del Direttore dell'Agenzia delle Entrate, è stato nuovamente differito il termine ultimo per l'adesione al servizio, possibile ora fino al 28 febbraio 2021, in quanto sono ancora in corso le attività di implementazione per recepire le disposizioni normative del Decreto-legge n. 124/2019. I soli dati fattura verranno mantenuti per le previste attività istituzionali di assistenza e di controllo automatizzato, fino a che non saranno decorsi i termini per gli eventuali accertamenti - ovvero entro il 31 dicembre dell'ottavo anno successivo a quello di presentazione della dichiarazione di riferimento. Con questo intervento al termine del periodo transitorio, l'Agenzia delle Entrate ha messo a punto il sistema di conservazione secondo le indicazioni del Garante.

Il rapporto fra contribuente e Agenzia delle Entrate

Analizzando la documentazione dell'Agenzia delle Entrate, un primo tema sul quale riflettere riguarda ruoli e responsabilità di due figure distinte: il **Responsabile della Conservazione** e il **Responsabile del servizio di conservazione**.

Il **Responsabile della Conservazione** viene indicato quale soggetto responsabile dell'insieme delle attività elencate nell'articolo 7, comma 1 delle regole tecniche del sistema di conservazione (DPCM 3/12/2013). Si tratta di un ruolo che richiede competenze tecnico-informatiche precise e non riveste natura solo formale.

Secondo l'Accordo di servizio il contribuente accetta il ruolo di Responsabile della Conservazione delle fatture per le quali richiede la conservazione all'Agenzia delle Entrate (art.1 D.lgs.127/2015) affidando la conservazione delle proprie fatture elettroniche mediante una delega parziale all'Agenzia delle Entrate (art.6, co.6 DPCM 3/12/2013).

Il **Responsabile del servizio di conservazione** viene individuato dall'Agenzia delle Entrate al proprio interno, ed è colui che definisce ed attua le politiche complessive del sistema di conservazione e ne governa la gestione, in relazione al modello organizzativo descritto nel Manuale del servizio di Conservazione.

Da quanto sopra esposto risulta quindi che:

- la responsabilità in ordine alla corretta conservazione dei documenti rimane in capo al contribuente;
- l'Agenzia delle Entrate opera in qualità di delegato del contribuente.

Il rapporto tra il contribuente e il soggetto delegato del processo di conservazione è stato analizzato dall'Agenzia delle Entrate, nella Risoluzione 161/E del 09 luglio 2007, nella quale si precisa che: *“in tutti i casi in cui il contribuente affida, in tutto o in parte, il processo di conservazione a soggetti terzi continuerà a rispondere nei confronti dell'Amministrazione Finanziaria della corretta tenuta e conservazione delle scritture contabili e di tutti i documenti fiscalmente rilevanti”*.

Eventuali inadempienze del soggetto incaricato della conservazione non potranno essere opposte all'Amministrazione Finanziaria per giustificare irregolarità o errori, quindi inadempienze compiute dall'Agenzia delle Entrate non sarebbero opponibili alla stessa, ma solo al contribuente.

I documenti conservati

Con l'accesso alla sezione “Dati rilevanti ai fini IVA” della propria area riservata il contribuente può visualizzare in formato leggibile i file xml delle fatture inviate e ricevute tramite il Sistema di interscambio, salvare il file xml in un proprio archivio, salvare i metadati del file xml inviato o ricevuto nel proprio archivio.

La conservazione proposta dal servizio dell'Agenzia delle Entrate riguarda le sole fatture emesse e ricevute in formato xml.

La durata del servizio di conservazione

Il servizio dell'Agenzia delle Entrate prevede espressamente un periodo di conservazione di 15 anni. Si tratta di argomento su cui porre particolare attenzione visto che i sistemi “commerciali” di conservazione prevedono condizioni contrattuali mutevoli a seconda della politica tariffaria del singolo conservatore e che vanno attentamente valutate in funzione delle esigenze di ciascuna azienda o professionista.

Il servizio di conservazione offerto dall'Agenzia delle Entrate risulta un utile strumento, per chi ha poche fatture da emettere e ricevere.

Ma chi ha necessità di avere un sistema di archiviazione integrato con procedure gestionali, verificando le scritture contabili formate sulla base di documenti digitali trasmessi e ricevuti, ha bisogno di ripensare i propri processi amministrativi, digitalizzandoli per ottenere risparmi economici e maggiore conformità alle vigenti normative.