BLOCKCHAIN E GDPR

Filosofia della Tecnologia e del Diritto

FILOSOFIA DELLA TECNOLOGIA E DEL DIRITTO

La tecnologia è uno strumento al servizio dell'uomo e come tale deve trovare un punto di allineamento con i principi e le regole di diritto.

*

***L'anarchia** è un concetto spaventoso per la maggior parte di noi ma sta insinuandosi nella nostra società da ogni angolazione, e la blockchain sta accelerando la tendenza. La blockchain tende a realizzare il **decentramento** e il decentramento consente l'anarchia.*

Nonostante non si conosca la vera identità di Satoshi Nagamoto, è certa la sua propensione all'anarco-capitalismo che si basa sul principio anarco-individualista di matrice libertaria secondo il quale, sul lungo periodo, i mercati, in assenza di un intervento statale, raggiungono autonomamente la situazione economica più efficiente).

Il termine "anarchia" ha connotazioni molto negative. La gente presume che implichi milizie armate nelle strade e hacker malintenzionati online, ma la vera definizione di "anarchia" è più ampia di quella. Si riferisce a una società che respinge ampiamente l'autorità a favore dell'autogoverno.

*

Il GDPR ha innalzato notevolmente il livello di tutela dei diritti e delle libertà degli individui in relazione al trattamento dei loro dati personali, introducendo anche una serie di obblighi e novità significative, dalla privacy by design e by default, agli obblighi di valutazione degli impatti privacy,

dall'accountability che passa anche attraverso la capacità del titolare del trattamento di scegliere le migliori tecnologie e misure di sicurezza al nuovo sistema sanzionatorio proporzionato.
La funzione del GDPR, come esplicitato nel testo, è di elevare "la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale" a diritto fondamentale. Si tratta di una questione di portata grandissima, e con risvolti potenzialmente enormi.
L'idea di fondo che ha ispirato l'introduzione della nuova normativa sulla privacy è quella di permettere che i cittadini europei abbiano <u>un controllo di gran lunga maggiore</u> sul modo in cui i singoli, le aziende e gli enti pubblici utilizzano le informazioni, e in particolare i dati sensibili, raccolti dagli utenti.
L'esigenza da cui è nato il GDPR, è quella di armonizzare e semplificare le norme riguardanti il trasferimento dei dati personali nell'Ue e per far fronte alle sfide date dagli sviluppi tecnologici.

1. Blockchain definizioni e funzionamento

La definizione di blockchain è ormai ben nota: si tratta di un data base distribuito (una sorta di registro delle "*transazioni*" dove i dati non sono memorizzati su un solo computer, ma su più dispositivi collegati tra loro via Internet, attraverso un'applicazione dedicata che permette di interfacciarsi con la "catena") fatto di blocchi di dati che memorizzano transazioni (non solo); per essere consolidato all'interno di un blocco, ogni dato, e successivamente ogni blocco prima di essere inserito nella "catena", viene sottoposto a un processo di **validazione.**

Prima di procedere all'analisi del funzionamente della tecnologia Blockchain dobbiamo prendere dimestichezza con due termini: nodi e miner. I primi possono essere individuati nei computer della rete che hanno scaricato la blockchain nella loro memoria; chiunque può diventare un nodo, tramite un apposito programma (ad esempio Bitcoin Core per Blockchain Bitcoin). I miner sono coloro che effettuano il controllo delle transazioni, grazie a computer molto potenti e attraverso un protocollo di validazione piuttosto complesso (spiegato più avanti), e il cui lavoro viene ripagato con un premio (il termine ormai condiviso per questa operazione è "minare", italianizzando il termine inglese to mine ossia estrarre).

Il protocollo di **validazione** (che definisce gli algoritmi validanti e chi può essere un miner) rappresenta dunque l'elemento vitale principale della blockchain perché è proprio da questo che dipendono sostanzialmente la velocità della catena e la sua sicurezza (gli algoritmi che governano questo processo non solo validano che ogni nuova immissione risponda a determinati criteri, ma impediscono anche che possano essere manomessi i dati già presenti nella catena). È dunque in questo ambito che si vedono le principali evoluzioni e che si differenziano, dal punto di vista tecnologico, le diverse blockchain. È comunque importante sottolineare che non necessariamente un protocollo è migliore di un altro: l'utilizzo dell'uno o dell'altro dipende anche dal tipo di

applicazione per la quale viene utilizzata la blockchain.

I principali protocolli di validazione sono:

1. Proof of Work – È il protocollo di validazione primigenio, sul quale si è basata la prima blockchain, Bitcoin, e a tutt'oggi ancora il più diffuso. Ogni 10 minuti un nuovo blocco, contenente migliaia di transazioni, viene immesso nella blockchain. La criticità di questo meccanismo risiede nella velocità per minare un blocco perché è un protocollo che, al crescere della blockchain, richiede sempre maggiore potenza elaborativa nei computer dei miner. Il tempo di validazione di una transazione (10 minuti) è uno dei motivi dal quale derivano le maggiori criticità in termini di scalabilità della tecnologia.

2. Proof of Stake – Nasce per far fronte al problema della scalabilità del precedente protocollo, semplificando il processo di mining. Il protocollo prevede inoltre che quando viene aggiunto un nuovo blocco venga automaticamente scelto il creatore del blocco successivo; per effettuare questa operazione di selezione vengono oggi utilizzati metodi diversi.

3. Federated Byzantine Agreement (FBA) – Se quelli descritti sono i due protocolli principali, ne sono stati poi creati altri, in parte derivazione di questi, in parte con elementi totalmente nuovi. Tra i più interessanti segnaliamo Federated Byzantine Agreement (FBA), sviluppato da Stellar Development Foundation (e utilizzato dalla seconda metà del 2015 dalla blockchain Stellar) basato su unità di fiducia (quorum slices) decise dai singoli server che insieme stabiliscono il livello di consenso del sistema

La blockchain è nata come modalità pubblica per effettuare transazioni (si tratta delle cosiddette blockchain unpermissioned o permissionless alle quali chiunque può accedere) ma la cd. Blockchain 2.0 vede il diffondersi di questa tecnologia (in ambiti diversi dalle criptovalute) sempre più all'interno di ecosistemi più o meno chiusi, con la conseguente nascita di blockchain private

Per meglio inquadrare le possibili applicazione della tecnologia Blockchain è necessario operare una distinzione tra:

a. blockchain pubbliche: tutti vi possono accedere e operare transazioni al suo interno o partecipare al processo di validazione. **Bitcoin ed Ethereum sono i più famosi esempi di blockchain pubbliche.**

b. blockchain private: controllate da **un'unica organizzazione che stabilisce chi può aderirvi**, chi può operare transazioni al suo interno e partecipare al processo di consenso/validazione

c. consorzi blockchain (permissioned): il processo di autorizzazione viene **delegato** a un gruppo preselezionato. La possibilità di aderire alla blockchain e di operare transazioni al suo interno può essere pubblica o limitata ai soli partecipanti. Questa tipologia di blockchain permissioned è particolarmente indicata per l'utilizzo nel mondo business.

2. Gdpr principi e regole

Il Regolamento Generale è entrato in vigore il 24 maggio 2016 ed applicato nei paesi Ue a partire dal 25 maggio 2018, dopo un periodo di transizione di due anni cambia radicalmente la filosofia e l'approccio della normativa al tema della DATA PROTECTION.

Si passa, infatti, da un sistema normativo di tipo formalistico (basato sulla previsione di regole formali e su un elenco di adempimenti e misure minime di sicurezza da adottare), ad un sistema di governance dei dati personali basato su un'alta responsabilizzazione sostanziale («***accountability***») del Data Controller (titolare del trattamento.

A quest'ultimo è richiesto in particolar modo **un approccio proattivo**, volto a prevenire (e non solo correggere) gli errori, nonché a dimostrare, anche documentalmente e/o tramite l'adozione di appropriate policy interne (da esibire in caso di richiesta da parte dell'Autorità), la conformità al GDPR e l'adeguatezza delle proprie scelte/valutazioni.

La maggiore discrezionalità per i Titolari del trattamento di decidere le modalità attraverso le quali conformarsi alle disposizioni del GDPR è gravata, inoltre, dall'onere di provare le ragioni che hanno portato a tali decisioni e le motivazioni alla base delle scelte effettuate.

Il nuovo Regolamento Europeo sulla protezione dei dati personali come detto prende le mosse da una prospettiva completamente diversa dal passato e pone l'accento sull'importanza che i dati stessi rivestono nel nostro sistema. Per comprendere la portata della nuova normativa si consideri che i dati personali vengono qualificati dallo stesso Regolamento come diritti fondamentali dell'uomo.

Il Regolamento punta su principi molto particolari che tendono a responsabilizzare il titolare del trattamento, il quale dovrà individuare le misure che garantiscano la protezione dei dati con riferimento alla sua situazione specifica.

Il GDPR introduce ad esempio i principi di privacy by design e privacy by default che impongono una rivoluzione nell'ambito della gestione dei dati.

Il Regolamento prevede la necessità di configurare il trattamento dei dati introducendo fin dall'inizio (ossia in fase di progettazione – by design) le garanzie indispensabili "al fine di soddisfare i requisiti" previsti dalla normativa e tutelare, in questo modo, i diritti degli interessati.

Tutto questo deve avvenire a monte, ossia prima di procedere al trattamento dei dati vero e proprio e rappresenta, quindi, un presupposto indispensabile per il corretto trattamento degli stessi.

Il principio di privacy by default, invece, impone l'adozione di misure tecniche e organizzative adeguate che siano per impostazione predefinita (di default appunto) quelle che garantiscono, in concreto nel singolo caso specifico, la tutela dei dati trattati.

3. Blockchain e Gdpr due mondi inconciliabili

La tecnologia Blockchain attrae sempre più gli operatori economici dalle banche ai trasporti, dalla sicurezza al fund raising.

Tuttavia, nonostante la popolarità, la sua applicazione pratica solleva molte domande, in particolare

per quanto riguarda la protezione dei dati personali oggetto del GDPR.

L'innovazione ma anche la problematicità di tale "paradigma organizzativo" deriva dal fatto che questo propone di trasmettere e memorizzare le informazioni su un immutabile registro decentralizzato, convalidato non da una tradizionale autorità centrale (come una banca o governo) ma dal "pubblico" stesso (nel caso della Blockchain permissionless).

Il fulcro di tale tecnologia consiste dunque nella decentralizzazione, trasparenza e immutabilità dei dati, concetti che ad un primo impatto sembrano scontrarsi con l'essenza stessa del GDPR. Se si riassumessero i 99 articoli del Regolamento in una sola parola sarebbe quella di **accountability** relativamente al trattamento dei dati personali.

L'idea sottostante tale Regolamento è infatti quella di responsabilizzare le organizzazioni, più precisamente il Titolare del Trattamento dei dati, riguardo ai rischi connessi all'elaborazione degli stessi.

Al riguardo, il GDPR elenca all'articolo 5 i sei principi essenziali alla data protection: il trattamento deve essere lecito, equo e trasparente; il trattamento dei dati deve essere limitato allo scopo specifico per il quale sono stati originariamente raccolti (limitazione di scopo); è possibile raccogliere solo i dati assolutamente necessari allo scopo specifico (minimizzazione dei dati); i dati devono essere accurati e aggiornati (accuratezza); i dati non devono essere conservati più a lungo del necessario (limitazione della conservazione); i dati devono essere elaborati in modo sicuro (integrità e riservatezza).

Le caratteristiche intrinseche della tecnologia Blockchain e della normativa UE sulla protezione dati determinano una lunga serie di interrogativi in merito alla loro compatibilità.

3.1. Lo stato delle tensioni tra Blockchain e GDPR

Prima di approfondire la nostra analisi ci sembra utile precisare che la maggior parte delle problematiche, in seguito affrontate, riguardano le Blockchain **pubbliche**, il cui esempio più famoso ci è fornito dai Bitcoin, le quali sono "aperte, senza proprietà e concepite per non essere controllate". Tutti i partecipanti possono ricoprire il ruolo di validatori. Al contrario le Blockchain definite come **private**, seppur strutturate sulla base di una logica decentralizzata, limitano l'accesso ad un numero ristretto di attori, i quali condividono rigorose norme e principi.

3.1.1. Difficoltà nell'identificazione del Data Controller: Il primo ostacolo che si pone al connubio Blockchain-GDPR è connesso alla differente distribuzione del peso nel controllo dei dati. Mentre il GDPR è concepito per applicarsi in un contesto fortemente centralizzato, l'essenza decentralizzata della Blockchain sembra scardinare l'idea stessa di controllo.

L'obiettivo in una Blockchain pubblica è quello di permettere a ciascuno di contribuire all'aggiornamento dei dati sul ledger ed impedire qualsiasi modalità di censura.

In tale contesto chi si pone nella condizione più adeguata per ricoprire il ruolo di Data Controller?

Si tratta dei protocol developers? Dei network users? Dei publishers of smart contracts?
Al riguardo, come verrà precisato in seguito, il CNIL francese sottolinea come non tutti i partecipanti ad una Blockchain possano ottenere tale qualifica. Ad esempio, una persona che vende o acquista Bitcoin per il proprio "account-wallet" non può ricoprire il ruolo di Data Controller.
Si prospetta una situazione differente, invece, se esegue tali transazioni nel corso di un'attività professionale o commerciale, per conto di altre persone fisiche. E' dunque raccomandabile adottare un approccio case-by-case.

3.1.2. Difficoltà nell'identificare la giurisdizione competente: Direttamente connessa a tale problematica vi è quella dell'individuazione della jurisdiction competente in caso di controversia relativamente al trattamento dei dati. Infatti, come attribuire la competenza ad una determinata giurisdizione se risulta impossibile identificare il responsabile del trattamento e il luogo in cui vengono elaborati? Anche riguardo a tale questione non vi sono al momento risposte certe e definitive.

3.1.3. Difficoltà nell'anonimizzare i dati personali: Il GDPR si applica al trattamento di dati personali a meno che questi non siano stati anonimizzati. L'anonimizzazione è il processo elaborativo che blocca la riconducibilità identificativa di dati personali con la persona alla quale si riferiscono. Bisogna dunque rendere impossibile l'identificazione di una persona e far in modo che tale operazione sia irreversibile.
E' in questa ultima caratteristica che si coglie la differenza con un concetto apparentemente simile: la pseudonimizzazione. Con tale termine si indica il processo che, se da una parte blocca la correlabilità dei dati personali all'identità di una persona, dall'altra non garantisce una possibile re-identificazione del soggetto interessato. Dunque un dato pseudonimo è ugualmente oggetto del GDPR, al pari dei dati personali.
Nel contesto Blockchain le operazioni di anonimizzazione risultano particolarmente ardue per la presenza di alcuni rischi:
–Rischio di inversione, ovvero la possibilità di invertire il processo e ricostituire i dati originali, ad esempio utilizzando il processo di brute force decryption.
–Rischio di linkabilità, ovvero il rischio che sia possibile collegare dati crittografati a un individuo, esaminando il contesto generale o confrontandoli con altre informazioni.
Finché la chiave esiste da qualche parte, i dati possono essere decifrati. Questo è particolarmente vero se consideriamo l'evoluzione costante della scienza della crittografia. Possiamo dunque prevedere, con una certa sicurezza, che le tecniche oggi utilizzate possano essere facilmente incrinate in futuro.

3.1.4. Difficoltà nella limitazione della conservazione dei dati: Il principio della conservazione

limitata dei dati incluso nel GDPR rappresenta un'ulteriore tensione alla sua coesistenza con la tecnologia Blockchain. Ai sensi dell'articolo 5 del Regolamento i dati devono essere conservati "per un periodo di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono trattati".

La tecnologia Blockchain, al contrario, risponde ad una logica completamente opposta, in quanto i dati, una volta scritti sulla catena non possono essere cancellati. Essi sono pertanto conservati a tempo indeterminato. L'immutabilità è una proprietà chiave della tecnologia. Anche se riuscissimo a identificare un Data Controller, sarebbe tuttavia impossibile tornare indietro e cancellare o aggiornare il report di una transazione senza distruggere la catena. Ne deriva che tale tensione non è esente neppure dalle Blockchain di tipo privato.

3.1.5. Difficoltà riguardo le questioni di territorialità: Il GDPR specifica all'articolo 45 che "il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato". Tale disposizione si scontra con l'essenza stessa della Blockchain pubblica in quanto, tenuto conto della molteplicità di partecipanti e della libertà di localizzazione inerente a tale tecnologia, risulta impossibile verificare che le garanzie siano state messe in azione. E' dunque complesso avere la certezza che i dati personali siano stati effettivamente trasferiti verso paesi considerati non "sicuri" dai Garanti europei. Se alcune soluzioni possono essere conseguite nel caso delle Blockchain private, grazie all'utilizzo di clausole contrattuali standard, norme vincolanti d'impresa, codici di condotta o meccanismi di certificazione approvati, nel contesto di una Blockchain pubblica la situazione risulta più problematica, dal momento che è difficile rintracciare la localizzazione dei partecipanti.

4. COMPATIBILITA'

4.1 Possibili tentativi per assicurare la compliance al GDPR

Nonostante le tensioni fin qui enumerate, non è possibile in alcun modo escludere l'esistenza di una possibile conciliazione tra questi due opposti.

La blockchain in realtà può giocare un ruolo fondamentale e proattivo del GDPR stesso, proprio a causa delle caratteristiche di immutabilità e replicazione. Progettato nel modo giusto, garantisce la necessaria trasparenza e controllo sui dati personali.

Infatti gli strumenti di crittografia e la struttura decentralizzata rendono la rete altamente resistente alla manomissione, in perfetta compliance con il GDPR. In aggiunta, la natura trasparente della Blockchain offre un accesso chiaro e diretto ai dati in linea con l'obiettivo di restituire il controllo e la visibilità degli stessi, proprio del GDPR.

Entrambi mirano a creare un ambiente in cui sia mantenuta la sicurezza dei dati e in cui sia ridato ai

soggetti il controllo sugli stessi. Se le intenzioni sono le medesime deve dunque esserci sicuramente un modo per arrivare ad una loro conciliazione.

1) Stoccaggio dei dati personali al di fuori dalla Blockchain

Una prima opzione potrebbe consistere nel memorizzare i dati personali al di fuori della Blockchain, iscrivendovi solo un collegamento di questi al loro interno, un hash dei dati (*si intende una stringa di lettere e cifre prodotta da una funzione di hash, vale a dire un algoritmo matematico capace di convertire una stringa contenente un numero variabile di caratteri in una seconda stringa, contenente invece una quantità fissa di caratteri. Anche una leggera modifica alla stringa di partenza può dare vita ad una hash totalmente diversa*).

Le Blockchain dovrebbero quindi essere utilizzate per archiviare la prova che alcuni dati esistono piuttosto che memorizzare gli stessi.

Ciò consentirebbe la rimozione dei dati personali senza rompere la catena.

Immaginiamo una piattaforma innovativa che utilizza una Blockchain pubblica per aiutare persone disoccupate a fornire la prova del loro background accademico a potenziali datori di lavoro. La piattaforma, invece di memorizzare direttamente tali rapporti scolastici (dati personali) sulla catena, potrebbe utilizzare tecniche di hash e di aggregazione per generare una prova dell'esistenza del report e archiviare questa nella Blockchain, insieme a un timestamp e alla firma crittografica dell'istituzione che ha generato il report. Successivamente la persona in cerca di lavoro mostrerà il rapporto scolastico al potenziale datore, il quale potrà confermare che questo è autentico grazie all'individuazione della firma e del timestamp nella blockchain. Questa seconda operazione avviene dunque off-chain.

In tal modo diventa anche concepibile l'esistenza di una sorta di diritto di rettifica. In effetti se si constata l'esistenza di un dato errato nel rapporto scolastico, questo può essere distrutto, essendo localizzato off-chain, e si può in seguito chiedere all'istituzione di generarne uno nuovo, il quale sarà identificato da una propria firma digitale nella Blockchain: "the previous digital signature will simply be 'left hanging', with no off-chain data to point to".

Sulla stessa linea di idee si iscrive la tecnologia utilizzata da Ethereum: "la filosofia alla base è la stessa dell'esempio precedentemente citato ovvero "non rivelare nulla tranne la verità dell'affermazione". Il vantaggio di tale strumento è che ciascuna parte è in grado di provare all'altra che ha un insieme specifico di informazioni, senza però rivelare quale sia il loro contenuto. I dati personali sono mascherati rendendo tale tecnologia perfettamente compatibile al GDPR.

2) Continuare ad investire sull'innovazione tecnologica

Come sottolineato dall'European Union Report, investire sugli sviluppi tecnologici potrebbe garantire un perfetto adeguamento della tecnologia Blockchain al GDPR, a lungo termine. Tra le innovazioni in corso d'opera si possono annoverare ad esempio delle speciali tecniche di

eliminazione che consentono di rimuovere i dati dalla blockchain una volta esaurito il loro obiettivo. Questa operazione non solo renderebbe il sistema più efficiente, in quanto sarebbero ridotte le dimensioni della catena, ma si porrebbe in perfetta compliance con l'articolo 5 del Regolamento.

Inoltre alcuni progetti stanno esplorando la creazione di tecniche di crittografia quantum-resistant, le quali non possono essere manomesse neanche attraverso l'uso di quantum computers. In aggiunta altri tecnici stanno analizzando l'uso dei 'chameleon' hashes (*una tecnica, chiamata "chameleon hash" (mappatura camaleontica) che aggiunge un lucchetto elettronico tra i diversi blocchi di una catena Blockchain, attribuendo a un amministratore la chiave digitale utile per sbloccarli e modificarli*). Tali hashes consentono di modificare i dati ad essi correlati. Infatti se un blocco associato con un hash deve essere modificato, vi è la possibilità di aprire tale blocco, cambiare il dato e rigenerare il blocco. Nonostante questa funzionalità non possa essere aggiunta retroattivamente a una Blockchain esistente, le sue prospettive per il futuro sono altamente positive.

A prima vista la tecnologia GDPR e Blockchain sembrano inconciliabili.

Il GDPR è stato concepito in un mondo centralizzato, mentre la tecnologia Blockchain rappresenta l'apoteosi della decentralizzazione. In relazione al Regolamento, abbiamo osservato che le sue caratteristiche cardine, come il diritto di rettifica e cancellazione, non possono essere facilmente applicate alle nuove tecnologie. Abbiamo tuttavia constatato che le Blockchain, se adeguatamente progettate ed il GDPR, possono condividere un obiettivo comune: dare ai soggetti un maggiore controllo sui loro dati. In questo specifico contesto, la sfida consiste nell'applicare il quadro di protezione dei dati dell'UE in modo tale da non asfissiare il potenziale innovativo delle Blockchain, ma allo stesso tempo garantire la protezione dei dati.

Dobbiamo essere disposti ad adeguare la legge al cambiamento tecnologico e ad accettare una maggiore interoperabilità tecno-legale. Ciò non significa che la protezione dei dati debba essere indebolita, ma piuttosto vale la pena esplorare se gli obiettivi del GDPR possono essere conseguiti attraverso mezzi diversi da quelli originariamente previsti. Le autorità di regolamentazione dovranno dunque spingere gli sviluppatori delle tecnologie Blockchain a progettare i propri prodotti in conformità con questo importante obiettivo di politica pubblica.

4.2. Le soluzioni del CNIL.

Vi sono ipotesi in cui il Titolare del trattamento deve valutare, fin dalla progettazione, se l'idea di business che egli intende implementare sulla piattaforma Blockchain sia compatibile o meno con la normativa europea.

In alcuni casi, quindi, le peculiarità caratterizzano la Blockchain (tra tutte: la decentralizzazione, la disintermediazione, e l'immutabilità dei dati), possono costituire un muro invalicabile in ottica di compliance normativa.

Si pone l'accento sul concetto di privacy by design e se ne comprende la portata: il GDPR ha

introdotto un modello di gestione del rischio, che necessita di progettazione e di misure preventive.
Per cui il tema della data protection va messo in cima all'agenda di chi crea e sviluppa una nuova applicazione tecnologica; il pericolo, altrimenti, è quello di realizzare un prodotto o un servizio non conforme – ab origine – rispetto ai principi di protezione dei dati personali, con tutte le conseguenze del caso in termini di costi e spese per porvi rimedio.

Questo il monito del CNIL.

Quali utenti Blockchain non sono da considerare titolari del trattamento?

I minatori (miners), vale a dire i nodi che convalidano le transazioni effettuate su piattaforma Blockchain; essi non entrano in contatto con i dati, nè condizionano l'oggetto delle transazioni; per cui non definiscono mezzi e finalità del trattamento ed anche gli utenti privati che trattano dati per scopi personali (es: chi compra o vende Bitcoin, anche per conto di terzi – salva l'ipotesi che l'attività di compravendita sia parte di un'attività commerciale e professionale).

Il Cnil ipotizza la adozione di soluzioni pratiche in caso di trattamenti effettuati da più utenti per una stessa finalità: individuare in anticipo il titolare del trattamento (es: creare una società o una qualche forma di associazione che funga da titolare; oppure identificare un utente che abbia il potere di prendere decisioni per tutti e designarlo titolare);

In caso contrario tutti potrebbero essere considerati contitolari ai sensi dell'art 26 GDPR; questo potrebbe generare confusione in termini di attribuzione di responsabilità (da una parte, gli interessati devono capire chi è il titolare di fronte al quale esercitare i propri diritti; dall'altra, l'autorità di controllo deve sapere chi è il soggetto che risponde di eventuli violazioni del Regolamento).

Quali utenti Blockchain possono rivestire la qualifica di responsabile del trattamento ai sensi dell'art. 28 GDPR ?

Gli utenti che trattano dati per conto del titolare - si pensi allo sviluppatore di un software che vende la sua nuova applicazione di smart contract ad una compagnia assicurativa – titolare del trattamento – permettendole di rimborsare automaticamente i passeggeri in caso di ritardo dell'aereo; in questo caso lo sviluppatore mette a disposizione il proprio servizio. Trattando i dati dei passeggeri solo per conto della compagnia assicurativa che avrà il controllo di quel trattamento, decidendone i mezzi (smart contract) e le finalità (utilizzo di dati personali a fini di rimborso).

Quale modello Blockchain pone maggiori criticità in ottica di compliance normativa?

Una Blockchain pubblica, nella quale chiunque può collegarsi per effettuare transazioni, pone questioni serie e complesse anche in materia di trasferimenti dati extra UE, non potendosi prevedere l'ubicazione dei nodi.

Cosa fare per conciliare il principio di minimizzazione e di limitazione della conservazione dei dati con il modello Blockchain?

Il CNIL raccomanda di valutare, fin dall'inizio, se le caratteristiche del modello Blockchain siano compatibili con le finalità del trattamento che si vuole effettuare; se l'esito è negativo, si consiglia di scegliere altre soluzioni che favoriscano la piena conformità al Regolamento europeo.

Per quanto concerne gli indirizzi degli utenti (identifiers of partecipants), questi sono da ritenersi essenziali per il corretto funzionamento dell'architettura Blockchain; ne consegue che gli stessi non potranno essere oggetto di ulteriore minimizzazione e che il loro periodo di conservazione dovrà necessariamente coincidere con la durata dell'esistenza della Blockchain.

I dati personali che non sono riconducibili ad utenti e minatori meritano di essere protetti con soluzioni tecniche e organizzative ad hoc: preferibilmente nella forma di un "commitment", un meccanismo crittografico molto complesso, che consente di "congelare" i dati in modo tale che sia possibile dimostrare alla controparte di aver eseguito tale operazione (da qui il termine "commit" inteso come impegno di una parte a non modificare o alterare i "dati congelati"), e che, dall'altra, non sia possibile ricondurre quei dati ad una persona fisica, utilizzando il solo "commit" (letteralmente: impegno o promessa); oppure mediante l'hashing dei dati, che è in grado di trasformare una qualsiasi quantità di dati in una stringa cifrata di dati di dimensioni fisse, denominata "digest".

I diritti dell'interessato sono compatibili con il sistema Blockchain?

Il CNIL opera necessariamente in merito un distinguo tra:

- diritti compatibili:
    - diritto di accesso;
    - diritto di portabilità.
- diritti difficilmente compatibili:
    - diritto alla cancellazione: non facilmente esercitabile nel sistema Blockchain, trattandosi di un registro immutabile. Vi sono tuttavia possibili soluzioni che si avvicinino allo scopo sottesso a tale diritto (es.: il titolare potrebbe rendere taluni dati praticamente inaccessibili, mediante l'utilizzo di algoritmi crittografici, raggiungendo, di fatto, gli effetti di una cancellazione);
    - diritto di rettifica: anche in questo caso bisogna tenere conto delle proprietà tecniche della Blockchain. Si potrebbe, ad esempio, inserire una nuova transazione che renda inefficace quella precedente, o comunque tale da rendere improduttiva quella precedente;
    - diritto di limitazione (nell'accezione di diritto di non essere sottoposto ad una decisione basata unicamente su un trattamento autorizzato): si pensi all'ipotesi di uno smart contract, cioè un programma in grado di essere eseguito in modo automatico, mediante la creazione di un processo guidato da algoritmi che non possono essere interrotti nè alterati a posteriori. In questo caso, si dovrebbe comunque consentire l'intervento umano, ad esempio permettendo

all'interessato di contestare l'effetto giuridico conseguente al trattamento automatizzato, una volta conclusosi il processo avviato dallo smart contract.

4.3. Le soluzioni dell'Osservatorio Europeo

L'Osservatorio ribadisce il supporto e l'importanza della blockchain come tecnologia ed osserva come non esistano cose tipo una blockchain che è conforme alle regole EU ("a GDPR compliant blockchain") e una blockchain che non lo è.

La GDPR tutela i dati personali e questi possono finire sulla blockchain.

Le tensioni tra blockchain e GDPR emergono almeno:

1.Quando la GDPR tutela le persone consentendo loro la rimozione o la modifica di dati personali (il nome forse più noto per questa possibilità è 'diritto all'oblio').

Possiamo fare qualcosa per l'immutabilità? Qui le cose si fanno più complesse. Non sembra si possano escludere diverse soluzioni: da time-stamped blocks (con cui, ad esempio, fornire una scadenza ai dati sensibili che, dopo tot, si distruggono) a soluzioni con più livelli (i dati sono on chain, però gli utenti sanno chi vuole vedere cosa e possono dare o meno l'autorizzazione a farlo).

2.Quando la GDPR definisce ruoli precisi relativi a chi controlla i dati e, quindi, è responsabile di effettuare eventuali modifiche.

Cercare di conoscere meglio la blockchain come tecnologia. Ad esempio, per quanto il nostro archetipo di blockchain (il network dei Bitcoin) sia decentralizzato non tutte le blockchain devono essere così aperte e permissionless. Una blockchain permissioned, in cui è presente una qualche forma di controllo sui nodi o su chi effettua il mining consente di individuare con più facilità quanto richiesto dalla GDPR.

Inoltre, il Report invita a considerare se e come la blockchain sia davvero necessaria per tutte le fasi del progetto, soprattutto per quanto riguarda la custodia dei dati personali.

La soluzione in questo caso diventa: tutto ciò che è passibile di tutela da parte della GDPR va messo off chain, la blockchain poi verrà integrate e utilizzata per il resto.

4.4 Adattare Blockchain per la conformità GDPR 08/08/2018

Sì, ci sono modi per le applicazioni Blockchain di essere conformi alle normative sulla privacy GDPR dell'Unione Europea.

La protezione dei dati e la privacy, tra gli altri, sono due importanti ragioni per l'entusiasmo globale attorno a Blockchain e perché la tecnologia sta trasformando il modo in cui transazioni affidabili, trasparenti e tracciabili si verificano su Internet.

Quindi è ironico che gran parte della reazione iniziale attorno a Blockchain relativa al regolamento generale sulla protezione dei dati (GDPR) è che la tecnologia è inadatta alle nuove direttive dell'Unione europea intese a migliorare la protezione e la privacy dei dati dei consumatori. Capita anche che si tratti di una miserigine superficiale e inutile. Uno sguardo più ravvicinato ai concetti e

alle tecnologie sottostanti di Blockchain rivela come la tecnologia migliora gli aspetti fondamentali della privacy e della sicurezza dei dati specificati in GDPR, a seconda di come questa soluzione è progettata per soddisfare le esigenze di GDPR.

La sfida fondamentale è l'adattamento della nuova tecnologia decentralizzata di Internet blockchain peer-to-peer per le direttive GDPR fondamentalmente basate sul tradizionale approccio Internet centralizzato.

Le tecniche alternative di Blockchain consentono l'implementazione orientata alla conformità GDPR. Queste tecniche richiedono un'approfondita comprensione delle tecnologie DLP (Blocked Distribution Ledger Technology) e del loro ecosistema. I processi di gestione delle identificazioni di Blockchain, come quelli che memorizzano e processano informazioni personali identificabili (PII), sono cruciali nella progettazione di soluzioni conformi a GDPR.

Uno dei principi chiave del GDPR è il "Diritto alla cancellazione" di 17 (o "Diritto all'oblio"). In base a questo principio GDPR, quando richiesto, i consumatori possono richiedere che le loro informazioni personali vengano cancellate dai loro elaboratori di dati (o "controllori").

Tuttavia, a causa del principio di "immutabilità dei record" di Blockchain, qualsiasi dato contenuto nelle transazioni di Blockchain è praticamente impossibile da modificare. I dati vengono copiati in nodi peer-to-peer, che funzionano come database distribuiti o registri distribuiti e sono i componenti principali della Blockchain. I dati che vengono aggiunti al pubblico, Blockchain senza autorizzazione è, infatti, lì per sempre, e, tecnicamente parlando, tali dati, o altri metadati, non possono essere modificati. A causa del modo in cui i blocchi Blockchain e le transazioni sono costruiti, tutte le informazioni e i record inseriti nei libri contabili distribuiti sono pubblicamente visibili, a prova di manomissione e immutabili.

Quindi, questa immutabilità delle transazioni di dati impresse nello stesso tessuto dei libri distribuiti rende Blockchain incoerente con l'articolo 17 di GDPR? Non necessariamente. L'adozione di architetture ibride off-chain per lo storage di dati distribuiti è un approccio alternativo per adattarsi a questa sfida. Altre alternative richiedono il mantenimento di dati PII all'interno dei dispositivi dell'utente, la creazione di metadati e hash di queste informazioni PII e il riferimento a questi dati locali utilizzando server di terze parti o lo stesso Blockchain. Questo crea diversi livelli di conformità Blockchain-GDPR.

Per rendere conto dell'articolo 17, quindi, un'alternativa è che tutte le informazioni e i dati sensibili al GDPR potrebbero essere archiviati fuori catena in server distribuiti o basati su cloud, con solo gli hash corrispondenti memorizzati nel livello Blockchain. In questo modo, gli hash fungono da indicatori di controllo per i dati sensibili al GDPR, che vengono memorizzati fuori catena. Questi puntatori di controllo non sono i dati dell'utente che GDPR cerca di proteggere, ma una pseudonimizzazione di quei dati originali. L'altro database che memorizza i dati originali non è, in

pratica, soggetto ai problemi riguardanti l'immutabilità dei record forniti da Blockchain. Ai fini della conformità dell'articolo 17, il fornitore di servizi può quindi cancellare la "linkabilità" del puntatore hash Blockchain ai dati presenti nei server off-chain distribuiti ogni volta che sia necessario.

Forse l'articolo più interessante - e più controverso - relativo all'applicabilità di Blockchain a GDPR è l'articolo 25, "Protezione dei dati in base alla progettazione e per impostazione predefinita", che affronta le tecniche di pseudonimizzazione per i dati memorizzati dei consumatori.

Hashing è la tecnica di pseudonimizzazione di Blockchain e ci sono due interpretazioni critiche per il collegamento pseudonimo usando Blockchain relativo all'articolo 25. Il primo afferma che, poiché la pseudonimizzazione dei dati viene eseguita nell'hash Blockchain, ma non nella anonimizzazione, il collegamento dati non è più considerato personale quando viene stabilito e, se questo collegamento viene eliminato, è anche conforme all'articolo 17. Tuttavia, la seconda interpretazione è che la pseudonimizzazione, anche con tutti gli hash crittografici, può ancora essere ricollegata ai dati PII originali. Tuttavia, potrebbe ancora essere necessario provare a livello matematico che il cyber-attacco a forza bruta del collegamento dati fuori catena utilizzando l'hashing può compromettere questa ipotesi.

La conclusione alla base di questa discussione è che questo problema rimane un obiettivo mobile poiché l'innovazione Blockchain sta accelerando, proprio come il GDPR è in fase di implementazione e sono in corso importanti battaglie legali-tecniche. Il regolamento GDPR deve adattarsi e accelerare rapidamente le ramificazioni, i problemi e le opportunità che consentono l'utilizzo di Internet decentralizzato di prossima generazione utilizzando la tecnologia Blockchain.

5. RUOLO DELLA BLOCKCHAIN IN OTTICA COMPLIANCE AZIENDALE

5.1. COMPLIANCE ALLA L. 231/01 : RAPPORTI TRA ODV E DPO

Con l’uscita del decreto legislativo 101/2018 che armonizza i contenuti del D.Lgs. 196/03 al più recente Regolamento europeo 679/2016 in materia di tutela dei dati personali, può essere utile una riflessione circa il rapporto tra la figura dell’Organismo di Vigilanza e quella del Responsabile della Protezione dei Dati.

Come è noto, gli illeciti legati a violazioni dei dati personali non rientrano esplicitamente nel novero dei reati per i quali si possa configurare la responsabilità dell’ente, motivo che potrebbe portare a considerare i due ambiti come compartimenti stagni. Ma se ci poniamo dal punto di osservazione dell’ente, le cose stanno in maniera diversa.

Il GDPR, infatti, richiede una valutazione dei rischi legati alla violazione dei dati personali trattati, per non menzionare l’eventuale valutazione di impatto aggiuntiva, esattamente come il D.Lgs. 231 01 richiede una valutazione dei rischi rispetto al coinvolgimento dell’ente nella commissione dei cosiddetti “reati presupposto”: e quando si arriva a parlare di reati informatici (solo per citarne uno),

alcune delle contromisure coprono evidentemente entrambi gli ambiti. Possono quindi cambiare il tipo di lenti indossate, ma gli occhiali dell'analisi di rischio ormai sono un accessorio che ogni ente deve mettere nel proprio libro cespiti, come del resto avviene anche nel mondo della normazione volontaria, in cui – solo per citare alcuni esempi – le norme in materia di sicurezza informatica (ISO 27001), salute e sicurezza dei lavoratori (ISO 45001) e qualità dei servizi erogati (ISO 9001) richiedono la conduzione di una analisi che renda il management consapevole dei rischi cui è esposto in modo da metterlo nelle condizioni migliori per prendere decisioni sulle contromisure da adottare.

O, in altri termini, che renda insostenibile la posizione per cui "non ero a conoscenza di questo rischio".

Se andiamo poi ad analizzare la figura del Responsabile della Protezione dei Dati (RPD, art. 37 del GDPR), tra i compiti che gli sono affidati rientrano "almeno" (art. 39) la consulenza sugli obblighi derivanti dal GDPR, la sorveglianza circa l'osservanza del Regolamento, la fornitura – se richiesta – di un parere in merito alla valutazione di impatto, in forte analogia operativa con quelli che sono i compiti ormai consolidati dell'Organismo di Vigilanza.

Rimane a questo punto una interessante domanda: i ruoli di OdV e RPD sono sovrapponibili? La risposta potrebbe essere sì – a meno di espliciti divieti normativi – ma è sottoposta ad almeno due condizioni. La prima è la competenza tecnica specifica per ambito: un conto è conoscere la responsabilità amministrativa e le sue implicazioni, un altro è la normativa in materia di tutela dei dati personali, dove oltre al Governo abbiamo la figura del Garante che dispone dell'autorità per normare direttamente la materia. Il membro dell'OdV che fosse anche RPD dovrebbe garantire un adeguato aggiornamento su entrambi gli ambiti. La seconda è la capacità di relazione: se l'OdV ha un ruolo di sicura interfaccia con le controparti interessate dal modello di organizzazione e gestione, il RPD (ancora una volta secondo l'art. 39) ha istituzionalmente quello di fungere da punto di contatto con l'autorità di controllo, con la quale è tenuto a cooperare. Se si pensa al tema delle segnalazioni circa le violazioni del modello o le lacune del sistema di controllo per la protezione dei dati (es. reclami) è più che auspicabile che le due funzioni, se fisicamente separate, cooperino strettamente per definire le specifiche regole di ingaggio.

In ultima analisi, le strutture degli ultimi dettati normativi mettono la Direzione dell'ente nella posizione facilitata di dover dialogare allo stesso modo con soggetti diversi, favorendo l'opportunità di investire in strumenti di gestione che consentano – se opportunamente tarati – la realizzazione di interessanti economie di scala, nonché di facilità di comprensione e attuazione da parte degli utenti. Non dimentichiamoci, infatti, che regole e controlli sia in ambito di responsabilità amministrativa che di tutela dei dati personali impattano direttamente sul lavoro quotidiano tanto del Megadirettore Naturale di fantozziana memoria quanto (rispettando la cinematografica similitudine) dell'ultimo

degli inferiori: e tanto più controlli e regole sono chiare, motivate e comprensibili, tanto più è alta la probabilità che vengano correttamente applicate.

E se consideriamo il rischio derivante dall'applicazione delle sanzioni nei due ambiti, non è un fattore da sottovalutare.

5.2. COMPLIANCE ALLA NORMATIVA ANTIRICICLAGGIO

Nell'ambito della Finanza Tecnologica o FinTech, la Blockchain rappresenta il percorso innovativo che gran parte delle Banche e gli altri Intermediari finanziari stanno esplorando per individuare la possibilità di utilizzo di tale tecnologia nelle procedure operative e organizzative, non necessariamente collegate alla gestione delle attività che ruotano intorno alle "criptovalute". Le Autorità Internazionali come l'EBA, la BCE, la Banca dei Regolamenti Internazionali, il FATF-GAFI e, di conseguenza, le Banche Centrali dei singoli Paesi, nel seguire l'andamento concitato della "escalation" tecnologica della Blockchain, sin dal 2013 hanno iniziato ad approfondire tale fenomeno diffondendo report, studi, statistiche e richiedendo ai "Regulators" una revisione delle normative antiriciclaggio vigenti, al fine di promuovere strategie atte a contrastare la diffusione delle valute virtuali in modo indiscriminato, nell'ambito di un sistema che, potenzialmente, favorisce l'anonimato generando così rischi legati al riciclaggio di denaro e al Finanziamento del Terrorismo. Con il passare del tempo, il sistema bancario, attraverso una valutazione più approfondita circa il funzionamento della Blockchain scollegato dalle criptovalute, ha individuato in questa nuova tecnologia un canale idoneo a svolgere funzioni per l'esecuzione di transazioni e altre funzioni interne organizzative come la Governance e AML. Il concetto di base dell'Antiriciclaggio prevede gli obblighi di identificazione e di valutazione del profilo di rischio associato al cliente e, quindi, ad esempio, per rendere attuabile lo scambio o la negoziazione delle valute virtuali in conformità alla regolamentazione vigente, si rende necessaria una normativa rigida e specifica riferita agli operatori del settore, finalizzata alla raccolta e tracciabilità delle informazioni sulle transazioni eseguite. La tecnologia Blockchain, se utilizzata nel settore finanziario, gestita con criteri e caratteristiche che ne consentono l'identificazione dei soggetti e la tracciabilità delle transazioni, compatibilmente con le prescrizioni antiriciclaggio e di contrasto al finanziamento del terrorismo, può rappresentare il nuovo scenario tecnologico, almeno in tale ambito normativo, che può essere utilizzato dalle Banche e dagli Intermediari Finanziari per agevolare la KYC "know your customer" della clientela, insomma una sorta di Grande Fratello per l'AML. L'esplorazione degli aspetti tecnici della Blockchain hanno portato a considerare la potenziale affidabilità del sistema per la conservazione delle informazioni e la tracciabilità delle transazioni. La transazione eseguita attraverso la piattaforma Blockchain condivisa, crittograficamente protetta, è assolutamente trasparente e la sua immodificabilità gli conferisce quel grado di sicurezza e tracciabilità che rappresentano gli elementi fondanti richiesti dalla normativa antiriciclaggio. Le Autorità di

Vigilanza, e Banche e gli altri Intermediari nell'intravedere le nuove prospettive di business e riduzione dei costi con l'applicazione della nuova tecnologia, hanno comunque la consapevolezza che, intraprendendo questo nuovo percorso, i rischi di "compliance" generati dalla "disintermediazione" sono amplificati e che le Autorità stesse dovranno individuare dei presìdi idonei a fronteggiare l'esigenza del rispetto delle normative di vigilanza nonchè la raccolta dei dati statistici per l'attuazione della politica monetaria. L'utilizzo della Blockchain per le finalità AML potrebbe essere paragonata ad una Biblioteca condivisa dalla quale possono attingere notizie solo gli "utenti abilitati"; le informazioni in essa custodite riferite al singolo cliente (KYC, profilo di rischio, sanzioni, etc) sono inserite, aggiornate e modificate a cura degli "utenti" stessi (Banche e Intermediari), ossia i medesimi soggetti che hanno accesso alle informazioni condivise necessarie per gli adempimenti connessi alla adeguata verifica della clientela. Pertanto, la Blockchain dovrebbe prevedere la distribuzione delle informazioni di identificazione digitale del cliente utente (predisposte da un gestore di firma digitale) attraverso i Provider di Servizio con i quali è in corso la transazione (Banche o Intermediari) sui registri condivisi dislocati presso i nodi che compongono la catena in modo tale che quella identità crittografata risulti da quel momento in poi comunque certificata e a disposizione di qualsiasi Provider di Servizio che intervenga nei rapporti con il cliente/utente nell'ambito di quella medesima Blockchain. In un sistema così strutturato è evidente che, fermo restando la assoluta garanzia circa l'inviolabilità della identità digitale, la Banca/Intermediario ne trarrebbe indiscutibili benefici che possono essere tradotti:

a) riduzione di tempi e costi per l'acquisizione delle informazioni, ovviamente previo assenso del cliente nel rispetto della Privacy;

b) miglioramento del rapporto con la clientela, evitando così continui fastidiosi contatti per l'acquisizione di documentazione cartacea;

c) riduzione dei costi legati alle verifiche della appartenenza a liste di embargo o antiterrorismo, attraverso la condivisione delle informazioni con altre parti che hanno già provveduto alle verifiche del caso.

La condivisione del KYC è un aspetto sul quale un gruppo di banche di livello internazionale sta attualmente sperimentando un sistema di identificazione digitale per persone fisiche e imprese condiviso attraverso la tecnologia Blockchain mettendo a punto controlli e verifiche di conformità alle normative di settore (privacy, sicurezza, AML). In termini di antiriciclaggio, più complessa appare la condivisione del profilo di rischio associato al cliente, inteso come un "rating" assegnato dalla banca di riferimento; il rating si basa sui criteri adottati da un intermediario e, gli stessi criteri, potrebbero non essere coerenti con quelli di un altro intermediario partecipante alla Blockchain provocando così una differente classificazione di rischio non utilizzabile, quindi, in termini di "condivisione". Certamente un dato crittografato con un rating di "profilatura" attribuito, basato su

un criterio univoco, consentirebbe una più agevole e immediata conoscenza del cliente per le finalità antiriciclaggio. La Banca d'Italia, nel corso di un Convegno del Giugno 2016, ha affermato che la "catena a blocchi" è attuabile purché con caratteristiche della c.d. Permissioned Ledger, quindi "non aperta" e nello stesso tempo controllata da attori individuati, con un sistema di convalida della transazione affidato ai Trusted; si tratta praticamente di un sistema affidato ad una Governance che stabilisce le regole del gioco e basato su un sistema di autorizzazioni. Un sistema anti-riciclaggio così impostato, sarebbe in grado di sfruttare la sicurezza delle informazioni crittografate, decentralizzate, quindi immutabili, per utilizzare tale tecnologia al fine di identificare e, eventualmente, bloccare le transazioni ritenute sospette.

Ogni Banca o altro soggetto tenuto all'osservanza della normativa antiriciclaggio che farà parte di questa Blockchain "Permissioned Ledger", fungerà da nodo all'interno della rete stessa e utilizzerà la directory di rete e i contratti intelligenti per registrare le transazioni nei registri condivisi presso gli altri "nodi". Poiché le informazioni pertinenti sarebbero archiviate nella blockchain e rese disponibili a ciascun nodo, l'attività sospetta può essere rilevata ed evidenziata a tutti i partecipanti correlati in modo tale che l'operatività riferita a quella posizione venga immediatamente sospesa e la rete blockchain verrebbe immediatamente e immodificabilmente aggiornata con la registrazione di tale circostanza. Una piattaforma antiriciclaggio strutturata in questo modo consentirebbe alle Autorità di Vigilanza, al Controllo Interno e ad altre parti interessate, di monitorare le transazioni in modo automatico, nonché di registrare immutabilmente la tracciabilità delle transazioni e delle operazioni sospette nel sistema. L'architettura della piattaforma, se realizzata conformemente alla regolamentazione, grazie all'elevato grado di automatismo di cui è dotata, rappresenta un ulteriore livello al presidio di controllo, trasparenza e tracciabilità delle transazioni. Una piattaforma globale basata sulla blockchain potrebbe essere utilizzata dalle istituzioni finanziarie partecipanti anche per una condivisione di informazioni relative alle transazioni potenzialmente fraudolente. Tuttavia, in un prossimo futuro, per una efficace realizzazione di un presidio antiriciclaggio che esprima appieno il proprio potenziale, le implementazioni di soluzioni basate su Blockchain devono necessariamente essere integrate nei programmi di sviluppo delle Information Technology aziendali attraverso una partecipazione programmata e condivisa con le Autorità Centrali.

Obblighi Privacy e Antiriclaggio Professionisti IV Direttiva

22 Agosto, 2017 Privacy

Con il recepimento della quarta direttiva antiriciclaggio, il D.lgs. 231/2007 ha subito notevoli modifiche, alcune delle quali hanno riflessi diretti sulle modalità di applicazione della normativa privacy all’interno dello studio professionale.

In particolare, il D.lgs. 231/07 così come modificato dal D.lgs. 90/2017, impone ai Professionisti (Commercialisti, Avvocati, Notai, Consulenti del Lavoro, Revisori Legali, Tributaristi e CED) di

adottare sistemi di gestione antiriciclaggio, che rispettino le prescrizioni dettate in materia di protezione dei dati personali dal D.lgs. 196/03 (Codice Privacy) e dal Regolamento Europeo Privacy UE/2016/679.

I Professionisti devono essere sempre in grado di garantire e dimostrare che il trattamento dei dati personali acquisiti nell'adempimento degli obblighi antiriciclaggio avviene per le sole finalità previste dalla legge antiriciclaggio e che i dati personali raccolti a tale scopo sono conservati separatamente dalla restante documentazione del cliente, nel rispetto delle prescrizioni dettate dal Codice Privacy e dal Regolamento Europeo Privacy.

I Professionisti, pertanto, sono obbligati ad adottare sistemi di conservazione della documentazione antiriciclaggio (cartacei o informatici) idonei a garantire il rispetto delle misure di sicurezza previste dal Codice Privacy e dal Regolamento Europeo Privacy e in grado di assicurare la tracciabilità dei soggetti legittimati ad alimentare il sistema di conservazione e autorizzati ad accedere ai dati personali e alle informazioni in esso contenuti.

Al fine di garantire un corretto trattamento dei dati personali, inoltre, i Professionisti sono obbligati a far frequentare a tutti i propri dipendenti e collaboratori corsi di formazione antiriciclaggio e privacy.

I programmi di formazione privacy e antiriciclaggio devono essere permanenti, avere carattere di continuità e essere in grado di innescare comportamenti positivi volti a garantire la conoscenza e il rispetto delle procedure antiriciclaggio e privacy dello Studio.

Nell’ambito dell’adempimento degli obblighi in materia di antiriciclaggio, i Professionisti, quindi, sono tenuti a rispettare le seguenti prescrizioni in materia di privacy:

Definizione di Organigramma Antiriciclaggio e Privacy

Nomina del Data Protection Officer (DPO)

Classificazione di dati e Trattamenti relativi agli obblighi antiriciclaggio

Analisi dei Rischi Privacy dei dati personali trattati per finalità di antiriciclaggio

Adozione di Misure di Sicurezza per la protezione dei dati personali trattati per finalità di antiriciclaggio

Informativa Privacy per il trattamento di dati personali per finalità di riciclaggio

Incarichi e Nomine Privacy per i soggetti che trattano dati personali per finalità di riciclaggio

Procedure e Istruzioni Antiriciclaggio e Privacy

Formazione Antiriciclaggio e Privacy

Istituzione e tenuta del Registro dei Trattamenti (Registro Privacy)

Audit e Verifiche Antiriciclaggio e Privacy periodiche

In caso di mancato rispetto degli obblighi privacy relativi agli adempimenti in materia di antiriciclaggio, il Regolamento Europeo Privacy (GDPR) prevede per i Professionisti Sanzioni

Amministrative Pecuniarie fino a € 20.000.000 o fino al 4% del Fatturato (ove superiore).

5.3. Compliance alla normativa su anticorruzione: l'esempio Spagna

L'OCSE stima che la corruzione negli appalti equivalga a $ 2 trilioni di fondi pubblici / contribuenti mondiali. Secondo un documento dell'OCSE, la tecnologia blockchain – portando trasparenza al processo di finanziamento degli appalti pubblici – può essere utilizzata come misura preventiva contro la corruzione che può distorcere l'equità nell'aggiudicazione degli appalti pubblici, ridurre la qualità dei servizi pubblici di base, limitare le opportunità di sviluppare un settore privato competitivo e minare la fiducia nelle istituzioni pubbliche.

L'UE, a febbraio ha lanciato l'Osservatorio e il Forum Blockchain dell'UE e ha già investito oltre 80 milioni di euro in vari progetti correlati. In qualità di membro della European Blockchain Partnership, la Spagna si impegna a creare blockchain e applicazioni di IA a livello UE che possano essere utilizzate nella lotta alla corruzione attraverso il mercato unico digitale a beneficio dei settori pubblico e privato.

Le applicazioni di blockchain più promettenti riguardano la registrazione e il tracciamento delle transazioni cripta-asset trasferite. Con il sostegno del Fondo europeo di sviluppo regionale, una società spagnola di blockchain sta sviluppando una soluzione di blockchain basata su Ethereum che permetterà alle parti di trasferire legalmente / contrattualmente la proprietà delle attività crittografiche riducendo le possibilità di manipolazione e frode, aggiungendo verificabilità e verificabilità alle transazioni digitali e tenendo traccia delle informazioni e delle risorse digitalizzate senza la necessità di intermediari. Il sistema incorporerà un'infrastruttura a chiave pubblica, come timestamp elettronici e servizi di consegna elettronica certificati, per tali contratti.

E se una risorsa crittografica venisse trasferita legalmente a un'altra in una transazione transfrontaliera corrotta? [19659008] Esempio: una società pubblica corrompe un funzionario straniero con un telefono ZTE che fornisce come minatore di criptovaluta e portafogli di criptovaluta. Ciò consente al funzionario straniero di estrarre Ethereum (ETH) in base alle necessità, vendere l'ETH estratto su uno scambio criptato e presentare all'azienda una bolletta dell'elettricità molto elevata per il rimborso delle attività minerarie, in cambio della prosecuzione degli affari nel paese straniero. Questa cosiddetta "nuova bustarella" elimina la necessità di banchieri, commercialisti, avvocati, consulenti e altri intermediari, rendendo così molto difficile il tracciamento e l'identificazione della "nuova tangente", soprattutto considerando che le leggi fiscali spagnole non richiedono l'estero o criptovalute custodite in portafoglio da dichiarare a fini fiscali. La "nuova bustarella" (qualcosa di valore) crea tuttavia la base apparente per una violazione FCPA. E se viene detratto a fini fiscali, potrebbe sottoporre la società che paga i tangenti a numerose multe e multe.

Per un'efficace corruzione e il rilevamento dell'evasione fiscale, i ricercatori dell'Università di Valladolid hanno sviluppato un'applicazione AI. Perché il primo passo nella lotta alla corruzione straniera e ai reati correlati, è la scoperta di esso. Il loro modello computerizzato si basa su reti neurali e calcola la probabilità di corruzione nelle province spagnole, nonché le condizioni che lo favoriscono. Questo sistema di allerta precoce analizza i dati da una varietà di fonti: province spagnole in cui casi reali di corruzione sono stati segnalati dai media o sono andati in tribunale tra il 2000 e il 2012; aumenti dei prezzi immobiliari; le tasse; crescita economica; il numero crescente di istituti di deposito e società non finanziarie; e lo stesso partito politico rimane al potere per lunghi periodi – per prevedere la corruzione pubblica basata su fattori economici e politici. Il punto è individuarlo il prima possibile, in modo che misure correttive e preventive possano essere prontamente adottate .

5.4. Compliance agli obblighi della cybersecurity

La blockchain è considerata inattaccabile dal punto di vista della sicurezza in quanto esente dall'intervento umano e grazie all'uso di chiavi pubbliche e private e di una criptografia asimmetrica. Ma non è proprio così e, come per altri sistemi, è necessario adottare controlli e standard di sicurezza.

Blockchain offre un approccio radicalmente diverso alla sicurezza informatica, che può arrivare a certificare l'identità di un'utente, garantire la sicurezza delle transazioni e delle comunicazioni e proteggere l'infrastruttura critica che supporta le operazioni tra le organizzazioni.

Un cambio di paradigma che può permettere di sfruttare al massimo i servizi online condivisi. Ma affinché questa tecnologia diventi davvero un catalizzatore di cambiamenti sociali e industriali, è essenziale chiarire i possibili impatti sulla sicurezza.

L'alto livello di dipendenza dalla tecnologia e da Internet ha portato oggi a nuovi modelli di business per le organizzazioni, ma ciò ha anche creato nuove opportunità da sfruttare per gli hacker, che si adoperano per sottrarre informazioni preziose (quali proprietà intellettuale, informazioni di identificazione personale, cartelle cliniche, dati finanziari) e monetizzano l'accesso ai dati mediante l'utilizzo di tecniche avanzate di ransomware o interrompendo le attività aziendali complessive tramite attacchi DDoS.

In questo contesto, la blockchain costituisce un supporto o un ostacolo per la sicurezza informatica?

La premessa ineludibile per parlare di sicurezza informatica si sviluppa attorno a tre elementi di base: confidenzialità, integrità e disponibilità, conosciuti anche con l'acronimo CIA (Confidentiality, Integrity, Availability).

Secondo l'Istituto nazionale degli standard e della tecnologia (NIST), la riservatezza dei dati si riferisce alla "proprietà che le informazioni sensibili non siano divulgate a persone, entità o processi non autorizzati". Proteggere l'accesso alla rete blockchain è fondamentale per garantire l'accesso ai

dati. Se un utente malintenzionato fosse in grado di accedere alla rete blockchain, aumenterebbero infatti le sue possibilità di riuscire ad accedere ai dati. Ne consegue che, analogamente ad altre tecnologie, i controlli di autenticazione e autorizzazione devono essere implementati anche nel caso di una blockchain. Sebbene tale tecnologia sia stata originariamente creata senza specifici controlli di accesso (a causa della sua natura pubblica), esistono alcune implementazioni blockchain che iniziano ad affrontare i problemi di riservatezza e controllo degli accessi, fornendo funzionalità di crittografia completa dei blocchi, che garantiscono che i dati non siano accessibili da parti non autorizzate mentre sono in transito.

Nelle blockchain pubbliche non è necessario controllare l'accesso alla rete poiché i protocolli delle catene consentono a chiunque di accedere e partecipare alla rete. Al contrario, le blockchain private richiedono l'esistenza di adeguati controlli di sicurezza per proteggere l'accesso alla rete. Si potrebbe supporre che reti e sistemi locali siano già ben protetti dietro il perimetro di un'organizzazione da diversi livelli di sicurezza interni (come firewall, reti private virtuali, VLAN, Intrusion Detection & Prevention Systems, ecc.). Tuttavia, pensare di affidarsi esclusivamente all'efficacia di tali controlli di sicurezza è chiaramente insufficiente. Per questo motivo, le best practice raccomandano che i controlli di sicurezza (come i controlli di accesso) siano implementati direttamente a livello applicativo, costituendo questa la prima e la più importante linea di difesa, specialmente nel caso in cui un attaccante riesca ad accedere alla rete locale o vi sia già presente. In linea con questi requisiti, la blockchain può fornire controlli di sicurezza avanzati, ad esempio sfruttando l'infrastruttura a chiave pubblica per autenticare e autorizzare le parti e crittografare le loro comunicazioni.

Se poi un utente malintenzionato accedesse ad una rete blockchain e ai suoi dati, non necessariamente sarebbe in grado di leggerne le informazioni.

La crittografia completa dei blocchi di dati può essere applicata ai dati in fase di transazione, garantendo in modo efficace la sua riservatezza. La crittografia end-to-end prevede che solo coloro che hanno l'autorizzazione ad accedere ai dati crittografati, attraverso la loro chiave privata, possono decifrare e vedere i dati. L'utilizzo delle chiavi di crittografia può fornire alle organizzazioni un livello di sicurezza più elevato. Ad esempio, l'implementazione di protocolli di comunicazione sicuri su blockchain garantisce che anche in una situazione in cui un utente malintenzionato tentasse di eseguire un attacco man-in-the-middle, non riuscirebbe a falsificare l'identità dell'interlocutore o a rilevarne i dati. Anche in uno scenario estremo in cui le chiavi private venissero compromesse, le sessioni passate verrebbero comunque mantenute riservate a causa delle perfette proprietà di protezione avanzata dei protocolli di sicurezza.

Sebbene gli utenti blockchain generalmente eseguano il backup della propria chiave privata in un luogo secondario, ad esempio in una cella frigorifera, il furto delle chiavi private rimane un rischio

elevato. In un ambiente aziendale sarà quindi fondamentale proteggere adeguatamente il materiale delle chiavi segrete in modo da non mettere a repentaglio il registro e lasciarlo confidenziale ed integro. Un esempio di protezione adeguata è l'uso di chiavi speciali che implementano tecnologie come i moduli di sicurezza hardware per proteggere i segreti principali e fornire un ambiente sicuro e resistente alla manomissione.

Le organizzazioni devono essere consapevoli che l'accesso al loro account blockchain da più dispositivi le sottopone ad un rischio più elevato di perdere il controllo delle proprie chiavi private. Devono quindi perseguire adeguate procedure di gestione delle chiavi (come le linee guida di gestione delle chiavi crittografiche IETF o RFC 4107) e sviluppare internamente procedure di governance delle chiavi sicure. Gli algoritmi crittografici odierni, utilizzati per la generazione di chiavi pubbliche e private, si basano su problemi di fattorizzazione di interi, che sono difficili da risolvere con l'attuale potenza di calcolo. I progressi nel campo dell'informatica quantistica diventeranno significativi per la sicurezza della blockchain a causa del loro impatto sull'attuale pratica di crittografia.

Ad esempio Bitcoin utilizza algoritmi crittografici per produrre una coppia di chiavi pubblica/privata ed un indirizzo che viene derivato utilizzando operazioni di hashing e checksum sulla chiave pubblica. L'esposizione dell'indirizzo da solo non è ad alto rischio. Tuttavia, l'esposizione dell'indirizzo e della chiave pubblica richiesta per la transazione, dati i progressi sufficienti nell'informatica quantistica, potrebbe permettere di derivare la chiave privata. Se il calcolo quantistico commerciale non è ancora disponibile come una realtà su larga scala, risulta importante pianificare ora il passaggio alla crittografia a resistenza quantistica. Non a caso, il NIST è attualmente impegnato nello sviluppo di standard di crittografia resistenti ai quanti.

Il NIST definisce l'integrità come la "protezione contro la modifica o la distruzione di informazioni improprie e include la garanzia di autenticità".

Garantire l'integrità dei dati durante l'intero ciclo di vita è fondamentale nei sistemi di informazione. Crittografia, confronto degli hash o utilizzo della firma digitale sono alcuni esempi di come i proprietari dei sistemi possono assicurare l'integrità dei dati, indipendentemente dalla fase in cui si trovano (in transito, a riposo o in uso).

L'immutabilità e la tracciabilità integrate delle blockchain forniscono già alle organizzazioni un mezzo per garantire l'integrità dei dati.

I protocolli del modello di consenso associati alla tecnologia presentano per le organizzazioni un ulteriore livello di garanzia sulla sicurezza dei dati, poiché in genere il 51% degli utenti di una blockchain deve accettare che una transazione sia valida prima di poter essere aggiunta alla piattaforma. Quando, infatti, c'è da comprovare una transazione, la maggioranza degli utenti deve essere d'accordo. Tuttavia, se si riuscisse a creare un gruppo di utenti e a controllarne il 50+1%, si

potrebbero creare delle transazioni truffa. Questo diventa chiaramente più semplice quando una blockchain è molto piccola o appena nata, pertanto è importante fare molta attenzione.

Anche gli smart contract forniscono un'ampia area di superficie per eventuali attacchi cyber. Blockchain introduce un nuovo paradigma nello sviluppo del software dei contratti intelligenti, per il quale standard e pratiche di sviluppo sicuri, come l'implementazione di codifiche e test di sicurezza, devono essere messi in atto per tenere conto del ciclo di vita del contratto intelligente, al fine di minimizzare la minaccia di un bug critico durante il ciclo di vita degli smart contract. L'attacco a The DAO, un'organizzazione decentrata costruita su Ethereum, è avvenuto proprio sfruttando un bug in un contratto intelligente, il che ha portato al furto di 60M Ether25.

Nel 2016, un aggressore ha sfruttato i contratti intelligenti di Ethereum per creare un overflow nella rete, fino al punto in cui la creazione di blocchi e la convalida delle transazioni hanno rallentato fortemente la rete.

La tecnologia blockchain non garantisce o migliora la qualità dei dati. Può solo assumersi la responsabilità dell'accuratezza e della qualità delle informazioni una volta entrate, il che significa che è necessario fidarsi che i dati estratti dai sistemi esistenti dell'organizzazione siano di buona qualità, alla stregua di tutti gli altri sistemi tecnologici. Un Oracle corrotto potrebbe quindi causare un effetto domino su tutta la rete e far sì che dati potenzialmente corrotti entrino in un ambiente sicuro. Visto che i dati verranno inevitabilmente trasmessi da un sistema di origine aziendale ad una blockchain, le organizzazioni devono garantire che i canali di scambio siano sicuri poiché questo è senza dubbio un punto di attacco e di ingresso per eventuali aggressori.

Il NIST definisce la disponibilità come "garanzia di accesso e uso tempestivo e affidabile delle informazioni".

Gli attacchi informatici che tentano di influire sulla disponibilità dei servizi tecnologici continuano ad aumentare. Gli attacchi DDoS possono causare interruzioni ai servizi Internet e alle soluzioni abilitate per blockchain. Gli effetti che ne derivano vanno dall'interruzione dei siti Web al mancato funzionamento delle App mobili, il che può generare perdite e costi ingenti per le imprese. Dato che le blockchain sono piattaforme distribuite, gli attacchi DDoS alle blockchain non sono regolari attacchi, in quanto tentano di sopraffare la rete con grandi volumi di piccole transazioni. Ed è prevedibile che gli attacchi DDoS aumenteranno ancora in futuro (in virtù del crescente numero di installazioni di dispositivi IoT poco sicuri, della disponibilità online di malware DDoS e di velocità di banda sempre più elevate) e produrranno attacchi regolari di Terabit/secondo in grado di mettere a dura prova la capacità dell'infrastruttura Internet regionale e persino globale. Va però sottolineato come le blockchain non presentino un singolo punto critico di vulnerabilità, il che riduce notevolmente le possibilità che un attacco DDoS basato su IP ne interrompa il normale funzionamento.

Se un nodo venisse rimosso, i dati sarebbero ancora accessibili tramite altri nodi all'interno della rete, poiché tutti mantengono una copia completa del libro mastro in ogni momento. La natura distribuita dell'infrastruttura blockchain fornisce un nuovo livello di accessibilità ai dati, attraverso uno qualsiasi dei nodi della rete, anche nel caso in cui un attacco DDoS interrompa alcuni di essi.

Anche se si ritiene che una rete blockchain non abbia in sé degli specifici punti di rottura all'interno del suo funzionamento, le organizzazioni potrebbero comunque affrontare rischi provenienti da eventi esterni al di fuori del loro controllo. Ad esempio, un'interruzione globale di Internet potrebbe interrompere anche una rete pubblica di blockchain distribuita come Bitcoin o Ethereum, creando interruzioni che potrebbero influire sulle operazioni di un'organizzazione, alla stregua di qualsiasi altra tecnologia.

La combinazione della natura peer to peer e del numero di nodi all'interno della rete rende la piattaforma resiliente dal punto di vista operativo. Dato che le blockchain sono costituite da più nodi, le organizzazioni possono rendere ridondante un nodo sotto attacco e continuare a funzionare come al solito. Quindi, anche se una parte importante della rete blockchain è sotto attacco, continuerà a funzionare a causa della natura distribuita della tecnologia.

La resilienza operativa della blockchain costituisce dunque un'area chiave da testare rigorosamente. Il management dovrebbe essere in grado di articolare i rischi principali connessi alla blockchain entro un sistema di governance e controllo stabilito per gestirli.

In conclusione, blockchain può contribuire a migliorare le tecniche di difesa cyber, prevenendo attività fraudolente attraverso meccanismi di consenso e rilevando la manomissione dei dati grazie alle caratteristiche sottostanti di immutabilità, trasparenza, verificabilità, crittografia dei dati e resilienza operativa.

Tuttavia, nessun sistema di difesa informatica può essere considerato sicuro al 100%. Ciò che è considerato sicuro oggi non lo sarà domani, per via della natura lucrativa del crimine informatico e a causa dell'ingegnosità dell'hacker criminale nel cercare nuovi metodi di attacco. Sebbene alcune delle funzionalità sottostanti delle blockchain riescano a garantire riservatezza, integrità e disponibilità dei dati, ciò non toglie che, proprio come per altri sistemi, sia necessario adottare comunque controlli e standard di sicurezza informatica per le organizzazioni che utilizzano le blockchain all'interno della loro infrastruttura tecnica, al fine di proteggere i propri dati da attacchi esterni