Blockchain e GDPR: riflessioni su alcuni elementi di contrasto

iusinitinere.it/blockchain-e-gdpr-riflessioni-su-alcuni-elementi-di-contrasto-43006
25/07/2022
Uncategorized
20/08/2022 redazione

Blockchain e GDPR: riflessioni su alcuni elementi di contrasto

a cura di Martina Franceschini. Articolo parte del progetto “Newsletter” di ELSA Perugia

La blockchain è oggi considerata la tecnologia maggiormente *disruptive* degli ultimi anni sebbene il suo funzionamento rimanga ancora oscuro per molti, complice l’elevato tecnicismo che la connota.

Prima di ragionare sulla compatibilità di questa infrastruttura con la normativa europea vigente sulla protezione dei dati (*General Data Protection Regulation* – GDPR), è utile descrivere e spiegarne i concetti fondanti.

Blockchain con la b minuscola e maiuscola

L’attenzione del mondo (non solo imprenditoriale) si è diretta verso questa nuova tecnologia (*rectius*, insieme di tecnologie) al fine di capirne il funzionamento e i vantaggi che possono derivarne per la collettività.

Nonostante sia possibile trovare le sue prime tracce in un tempo risalente[1], il suo creatore è comunemente rinvenuto nella figura di Satoshi Nakamoto, personaggio rimasto anonimo e oggetto delle più curiose speculazioni. Nel suo *white paper****[2]***, pubblicato nel 2008, Nakamoto ha chiarito universalmente il metodo di funzionamento e l’ha indissolubilmente legata alla criptovaluta di sua invenzione, il Bitcoin, ponendo le basi verso una progressiva esclusione degli intermediari nei pagamenti elettronici e costruendo un sistema di scambi commerciali *peer-to-peer*.

Nonostante siano passati quattordici dal manifesto di Nakamoto, ad oggi, risulta ancora difficile comprendere la blockchain e gli applicativi che vi ruotano attorno, perciò cercheremo di dare definizioni semplici, senza addentrarci negli aspetti più tecnici.

Serve tuttavia una precisione sul termine “blockchain”: in quanto blockchain originale, quando ci si riferisce alla blockchain di Bitcoin (e quindi di Nakamoto) si utilizzerà la b maiuscola; quando invece, ci si riferisce alla tecnologia si utilizzerà la b minuscola.

Dal punto di vista normativo, la legge n. 124 del 2019, all’articolo 8*ter*, definisce le blockchain come le “tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato

su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da critto-grafia verificabili da ciascun partecipante, non alterabili e non modificabili"[3].

Sulla base della definizione appena riportata, la blockchain appartiene alla più ampia categoria dei sistemi DL (*Distributed Ledger*) cioè dei registri distribuiti, consultabili da tutti i partecipanti di una rete. Questi registri sono formati da catene di blocchi – come suggerisce il nome stesso – contenenti un insieme di informazioni.

Ogni blocco, quindi, non è altro che un insieme di dati[4], la cui provenienza ed ora di esecuzione non possono essere modificate, grazie all'utilizzo della crittografia (asimmetrica) e del *timestamping*[5]. Inoltre, il blocco precedente si lega al blocco successivo grazie a un codice alfanumerico di lunghezza predeterminata (funzione di *hash**[6]***) che include anche l'*hash* del blocco anteriore, formando così una catena inscindibile e non mutabile.

Gli attori principali che risiedono sulla blockchain sono i nodi – fisicamente costituiti da server – che hanno libertà di controllare le transazioni presenti sul registro.

In particolare, vi sono specifici nodi (*miner*) che si occupano di validare le transazioni contenute nei singoli blocchi, consentendo così di condividere su ciascun nodo l'intero archivio di transazioni generatosi fino a quello specifico momento, senza ricorrere a un'autorità centrale.

La validazione può avvenire con modalità differenti in base al tipo di meccanismo di consenso previsto dal protocollo[7].

Il più conosciuto è il *Proof of Work* (d'ora in poi PoW) che caratterizza la Blockchain di Bitcoin. Il PoW si basa su una vera e propria sfida computazionale tra nodi, i quali cercano di risolvere un puzzle crittografico nel minor tempo possibile, cercando di battere sul tempo gli altri nodi. Il primo nodo che trova soluzione all'interrogativo potrà sottoporre la soluzione alla rete e – se ottiene la maggioranza dei consensi – validare il blocco e ricevere un premio per il proprio lavoro.

Al fine di superare gli inconvenienti della PoW[8], altre blockchain hanno sviluppato una modalità di validazione alternativa: la *Proof of Stake* (PoS). In questo caso, la capacità di calcolo del server è irrilevante poiché la PoS si basa sulla quantità di liquidità fruita dal nodo.

In sostanza, la possibilità di validare blocchi è proporzionale alla quantità di *criptoassets* posseduta dal nodo in quella specifica blockchain. La *ratio* che fonda la PoS si poggia su una banale valutazione degli interessi: un *miner*, che dispone tanta liquidità da avere il diritto di validare blocchi, non ha alcun interesse ad attaccare il network con validazioni mendaci perché questo comportamento fallace finirebbe per colpire maggiormente chi – come questo – possiede più cripto valute in circolazione[9].

Per concludere, serve riferirsi anche ai tipi di blockchain esistenti oggi, che si differenziano in base alla presenza di un'entità terza in grado si selezionare i partecipanti.

Schematizzando, possiamo annoverare[10]:

[11][12][13]
I vantaggi che questa tecnologia è in grado di garantire sono – oltre alle già citate decentralizzazione e disintermediazione – la trasparenza (il registro è diffuso su tutto il network), l'immutabilità dei dati registrati e la tracciabilità dei trasferimenti[14].

Il GDPR e la tutela dei dati personali

Il GDPR è il più recente tassello del percorso comunitario di tutela dei dati personali iniziato nel 1995 con la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati), che ha avuto il merito di sancire per la prima volta le regole sulla circolazione dei dati personali in Europa – successivamente precisati da ulteriori direttive[15]. La frammentazione normativa di quegli anni, fu superata nel 2016, con l'emanazione del Regolamento sulla protezione dei dati personali (GDPR), progettato per armonizzare le esigenze di protezione e circolazione dei dati personali.[16]

Tra le novità più importanti introdotte dal GDPR, vi è l'enunciazione di principi fondamentali regolatori della materia, di cui si tratterà tra poco[17].

Da questo breve excursus storico, è evidente che la protezione dei dati personali ha sempre rappresentato un obiettivo politico fondamentale per l'Unione Europea[18] anche in tempi in cui i dati non avevano ancora assunto il ruolo di attuale predominanza[19].

Il regolamento 2016/679[20] rappresenta il corpus normativo in vigore con maggior rilevanza nel panorama europeo ed è ad oggi il punto di riferimento in tema di protezione dei dati personali. Tuttavia, essendo stato redatto anni prima della reale ascesa della tecnologia blockchain, sarà necessario ragionare, nei successivi paragrafi, sulla possibilità di coordinamento tra la normativa e la nuova tecnologia.

Innanzitutto, serve chiarire cosa sia un dato personale.

È lo stesso Regolamento[21] a fornire una definizione, precisando che dato è "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)". I dati, perciò, sono tutte le informazioni strettamente correlate alla persona e che vanno oltre il – banale – nome e cognome, riferendosi anche ad abitudini, stili di vita, relazioni personali ecc.[22]

Il GDPR individua precisamente il ruolo e i compiti dei soggetti coinvolti nella protezione dei dati personali, consistenti – oltre l'"interessato" – nel "titolare del trattamento" e "responsabile del trattamento".

Cercando di descrivere in modo semplice queste figure, possiamo così inquadrarli:

- **interessato**[23]: è il soggetto fisico a cui i dati sono riferiti;
- **titolare del trattamento**[24]: è la figura chiave ("persona fisica o giuridica, autorità pubblica, servizio o altro organismo che… determina le finalità e i mezzi del trattamento") in tema di protezione dei dati perché è a questo soggetto a cui l'interessato si rivolge per far valere i propri diritti riconosciuti dal regolamento[25];
- **responsabile del trattamento**[26]: è la persona (fisica o giuridica) che compie il trattamento dei dati, rispondendo direttamente al titolare.

Il modello tracciato dal GDPR appare centralizzato[27], prevedendo che sia un soggetto ben definito – il titolare – a occuparsi del trattamento dei dati. Da ciò consegue che, nel caso di violazioni della normativa, questo diviene direttamente responsabile nei confronti dell'interessato.

Ciò posto, non è difficile notare che la centralizzazione sia diametralmente opposta ai caratteri integranti la blockchain. Nondimeno, abbiamo già evidenziato il decentramento e l'assenza di intermediazione di questo gruppo di tecnologie: l'archiviazione ed elaborazione dei dati avviene su ogni nodo e non è rimessa ad una autorità centrale.

Il titolare del trattamento nella blockchain

Il primo problema che si pone riguarda l'individuazione del titolare del trattamento nella blockchain.

Il principio di *accountability* (responsabilità) designato dal GDPR, rileva non solo nel caso di violazione della normativa, ma anche nella fase preventiva, nella quale spetta al titolare scegliere le "misure tecniche e organizzative"[28] utili a evitare le manomissioni esterne (tali doveri si intrecciano con i concetti di *privacy by design* e *privacy by default****[29]***).[30]

Per individuare il titolare del trattamento nelle blockchain serve tornare alla distinzione tra private e pubbliche.

Nelle prime, sembrerebbe più facile individuare un titolare del trattamento, dal momento che l'accesso è vincolato all'autorizzazione di determinati soggetti. Perciò si replicherebbe una sorta di governo centralizzato che ben si sposa col prototipo disegnato dal GDPR[31].

Diverso e più complesso è il caso delle blockchain *permissionless*, dove tutti possono partecipare e interagire senza vincoli (schema peer-to-peer) e non è possibile trovare un unico punto di controllo del network.

Partendo dalla lettera della norma, sembrerebbe condivisibile la tesi di chi esclude che i *miners* siano titolari del trattamento: il titolare deve determinare le finalità e i mezzi del

trattamento, compiti che fuoriescono dall'attività del *miner*, il quale si limita a eseguire il protocollo per vincere un premio, qualificandosi come mero soggetto passivo[32]. Inoltre, se si ammettesse tale possibilità, sarebbe assai difficile per l'interessato rivolgersi alla totalità dei *miners* per far valere i propri diritti, considerata la difficoltà di conoscere il reale numero dei nodi sulla rete.

Per i medesimi motivi, appare facilmente superabile la tesi di chi sostiene che titolari del trattamento potrebbero essere gli sviluppatori del protocollo: questi, difatti, si occupano solo di costruire un'infrastruttura tecnologica per altri *users*.

Secondo altri, la figura del titolare sarebbe incorporata dalla totalità dei nodi della rete[33]: precisamente, il nodo che immette dati nel network incorporerebbe sia l'utente che il titolare del trattamento, mentre, nel caso si limiti a riceve tali dati, risponderebbe solo in qualità di responsabile. Anche questa tesi non rimane esente da critiche, concernenti principalmente l'impossibilità di adempiere al principio di *accountability* in assenza di strumenti che permettono il monitoraggio sull'utilizzo dei dati.

Infine, c'è chi sostiene che i titolari del trattamento non siano i nodi, bensì gli *users* (chi compie concretamente le transazioni). In tal caso, se l'*user* utilizzasse la blockchain per scopi personali[34] (non attività commerciali) non dovrebbe applicarsi il GDPR ex articolo 2, comma 2, lettera c.[35]

Principi e diritti del GDPR

Come annunciato, vi sono altre problematiche da vagliare nel rapporto con la blockchain, in particolare, quelle che concernono i principi fondanti del Regolamento (articolo 5) e alcuni diritti riconosciuti all'interessato.

Il primo principio[36] si presenta composito poiché comprende i principi **di legalità, equità e trasparenza**. Ciò presuppone che il titolare del trattamento debba avere motivi legittimi per raccogliere i dati, trattandoli in modo trasparente e senza commettere attività illecite. Se la trasparenza è di certo soddisfatta nella blockchain, lo stesso non può affermarsi in merito al principio di legalità, poiché un uso è lecito solo quando sussiste una delle condizioni dell'articolo 6. Se prendiamo l'esempio del consenso, viene spontaneo domandarci a chi presti il consenso l'utente quando rimane ancora incerto chi sia il titolare del trattamento.[37]

Il principio di minimizzazione dei dati[38] prevede che questi siano "adeguati pertinenti e limitati" e utilizzati solo per le finalità dichiarate. Inoltre, devono essere "**esatti**, e se necessario, aggiornati"[39] e il titolare deve porre in campo tutte le misure idonee a modificare/cancellare tempestivamente i dati quando ciò sia richiesto dall'interessato. Anche in questo caso, non è difficile immaginare un'incompatibilità con la blockchain, dato che si caratterizza per essere un sistema di sola aggiunta[40], per cui un dato (anche errato) rimane su tutti i blocchi della catena perennemente, senza possibilità di modifica o cancellazione. La blockchain, per sua natura, è destinata a crescere e non

può in alcun modo regredire, ed è proprio l'immutabilità dei dati a giustificare la fiducia della rete.

L'immodificabilità delle informazioni si pone in diretto contrasto con il **diritto di rettifica e integrazione**[41] dell'interessato. Difatti, anche se si superassero le difficoltà in ordine all'individuazione del titolare, questo non potrebbe in alcun modo modificare la catena di blocchi. Al massimo, potrebbero aggiungersi nuovi blocchi con dati rettificati.[42]

Allo stesso modo, le caratteristiche appena esaminate contrastano anche con il **diritto all'oblio**[43], che include sia il diritto di cancellazione che il diritto all'oblio vero e proprio[44]. Se il primo riguarda il potere di cancellare i dati ricevuti da parte del titolare del trattamento, il secondo obbliga i terzi, anche loro destinatari di dati, a eleminare qualunque copia o riproduzione dei dati personali. L'immutabilità della catena pone gli stesi dubbi che abbiamo appena analizzato per il diritto di **rettifica**. Tuttavia, la legge prevede che si tenga conto "della tecnologia disponibile e dei costi di attuazione" prima di procedere alla cancellazione, riferimento che permetterebbe di giustificare l'impossibilità di esercitare tale diritto su blockchain. [45]

Anche il diritto di **accesso[46]** – articolo 15, GDPR – va ridimensionato a causa delle caratteristiche della blockchain, poiché appare complicato poter consultare i dati registrati su blockchain quando questi sono cifrati.

Pseudonimìa e anonimìa dei dati

L'ultima problematica riguarda l'applicabilità del GDPR ai dati **pseudonimi** e **anonimi**. Secondo il Considerando n. 26[47], il Regolamento è applicabile ai dati **pseudonimizzati**, "i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni", ma non alle informazioni **anonime**, cioè non riferibili "a persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".

La pseudonimizzazione consiste nella sostituzione di un dato con un altro, così da evitare l'identificazione del soggetto, il quale rimane identificabile ma non tramite quello specifico dato. Alcuni dei metodi che garantiscono la pseudonimia sono rinvenibili nella funzione di *hash* o nel sistema di chiavi asimmetriche[48] (pubblica e privata). Tuttavia anche se non idonei a permettere l'identificabilità, i dati pseudonimizzati[49] inseriti su blockchain, tramite la funzione di *hash*, sono comunque da ritenere dati personali, con il conseguente obbligo di applicarvi le regole del GDPR.[50]

Al contrario, non è chiaro se le chiavi pubbliche registrate su blockchain rientrino in questa categoria. Nonostante la diversità di opinioni, pare plausibile sostenere che anche le chiavi pubbliche utilizzate su blockchain facciano parte della categoria dei dati personali perché non sono in grado di garantire l'irreversibilità dell'identificazione. La pseudonimia, quindi, non assicura all'interessato la totale schermatura della propria identità poiché sarebbe sempre possibile risalirvi grazie alla chiave pubblica e all'insieme di tracce che ogni soggetto lascia sul *web*. [51]

Conclusioni

Dall'analisi appena condotta, si è evidenziato come la blockchain sia una tecnologia, per definizione, incapace di dimenticare e resistente alla censura grazie al suo modello di archiviazione diffusa dei dati. Sono proprio queste caratteristiche ad aver determinato la sua ascesa negli ultimi anni, in combinazione con la sua profonda versatilità, che la rende adatta a essere utilizzata in molteplici campi.

In questi anni abbiamo visto crescere l'attenzione anche verso altre esigenze, altrettanto importanti e strettamente connesse all'avanzare dell'innovazione. La protezione dei dati personali è difatti una priorità europea (e nazionale) addirittura precedente alla creazione di Nakamoto, la quale ha determinato l'insorgenza di problematiche sull'applicabilità della normativa europea a questa infrastruttura tecnologica e ha determinato l'esigenza di trovare un coordinamento tra questa e il vigente modello normativo.

Nonostante alcuni aspetti e alcuni diritti riconosciuti dal Regolamento non siano di facile attuazione, è chiaro che esista spazio di manovra per rendere la blockchain *compliant* al GDPR. Oltretutto, non si deve dimenticare che tale normativa e la blockchain hanno la potenzialità di procurare all'interessato/utente un maggior controllo dei suoi dati[52].

La sfida che ci attende nei prossimi anni concerne la necessità di trovare un equilibrio tra due esigenze di matrice europea (e nazionale): supportare l'innovazione evitando di costringerla all'interno di un quadro normativo inflessibile e al contempo garantire la protezione dei dati personali anche di fronte all'avanzare delle nuove tecnologie[53].

In conclusione, non può affermarsi che questa tecnologia sia in assoluto incompatibile con la normativa vigente sulla protezione dei dati, ma semmai che l'uso fattone finora è risultato di difficile coordinamento in alcuni casi e per alcuni aspetti. Tuttavia, come già affermato, date le enormi potenzialità che si registrano in ambito blockchain, ci auspichiamo che il legislatore lavori in questa direzione.

[1] È interessante ricordare la storia dell'isola di Yap, dove, già nel 500 d.C., è possibile rinvenire le prime tracce di metodologie di pagamento simili alle attuali monete virtuali, come Bitcoin. Di fatti, gli abitanti dell'isola utilizzavano come monete di scambio delle pietre di notevole diametro e pesanti svariate tonnellate. Data la grandezza, trasportare fisicamente la pietra da un acquirente all'altro risultava impossibile, perciò fu necessario ricorrere a soluzioni diverse per tenere traccia degli scambi. Fu così che ciascun possessore della pietra si dotò di un proprio registro, nel quale annotare (contestualmente a tutti gli altri possessori di registri) ogni transazione, cioè ogni cambio di proprietà della pietra/moneta.

Vedi nello specifico, Berentsen A., Schär F., *A short introduction to the world of cryptocurrencies*, https://files.stlouisfed.org/files/htdocs/publications/review/2018/01/10/a-short-introduction-to-the-world-of-cryptocurrencies.pdf.

[2] S. Nakamoto, A peer-to-peer electronic Cash System, https://bitcoin.org/bitcoin.pdf.

[3] Legge n. 12/2019 rubricata “Conversione in legge, con modificazioni, del decreto legge 14 dicembre 2018, n. 135 recante disposizioni in materia di sostegno e semplificazioni per le imprese e per la pubblica amministrazione”.

[4] Se si trattasse di Bitcoin, il blocco conterrebbe tutte le informazioni che riguardano quella transazione di criptovaluta, cioè la quantità di moneta trasferita nonché i dati del mittente e del ricevente

[5] L. Parola, P. Merati, G. Gavotti, *Blockchain e smart contract: questioni giuridiche aperte*, p. 681.

[6] La funzione di hash è una tecnica matematica che genera come output una stringa di caratteri univoca e di lunghezza predeterminata, indipendentemente dalla quantità e qualità di dati inserita (input).

[7] Il protocollo rappresenta le regole, condivise dai nodi, che definiscono il funzionamento della blockchain (dimensione dei blocchi, meccanismo di consenso ecc. ecc.).

[8] È l’algoritmo di consenso alla base della Blockchain che consistite nella risoluzione di complesse operazioni di calcolo da parte del *miner* e sottoposte all’approvazione della rete, così da permettere l’aggiunta di un nuovo blocco al regisro.

[9] R. Garavaglia, *Tutto su blockchain. Capire la tecnologia e le nuove opportunità*, pp. 67 ss.

[10] Ibid, pp. 117 ss.

[11] L’esempio di blockchain pubbliche più noto riguarda Ethereum e la Blockchain di Bitcoin.

[12] Un esempio è fornito da Hyperledger Fabric.

[13] Sono poco conosciute ma rimangono un esempio calzante le blockchain Hyperledger Sawtooth e Ripple.

[14] https://blog.osservatori.net

[15] Direttive 2002/58/CE e 2009/136/UE.

[16] The European Union Blockchain Observatory and Forum, Blockchain and the GDPR report, https://www.eublockchainforum.eu/

[17] L. Ibanez, K. O'Hara, E. Simperl, *On Blockchains and General Data Protection Regulation*, p.3, https://www.researchgate.net/publication/326913146_On_Blockchains_and_the_General_Data_Protection_Regulation

[18] La protezione dei dati personali è sancita nella Carta europea dei diritti fondamentali, all'articolo 8, http://fra.europa.eu/en/charterpedia/article/8-protection-personal-data.

[19] Nel 2006, Clive Humby, matematico e data scientist inglese, coniò lo slogan "i dati sono il nuovo petrolio".

[20] 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, consultabile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679

[21] Articolo 4, comma 1, n.1, GDPR.

[22] https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali

[23] Articolo 4, comma 1, n.1, GDPR.

[24] Articolo 4, comma 1, n. 7, GDPR.

[25] The European Union Blockchain Observatory and Forum, Blockchain and the GDPR report, https://www.eublockchainforum.eu/, p.11.

[26] Articolo 4, comma 1, n.8, GDPR.

[27] M. Finck, Blockchains and Data Protection in the European Union, Max Planck Institute for innovation & Competition Research paper, n. 18-01, https://edpl.lexxion.eu/article/edpl/2018/1/6

[28] Articolo 32, GDPR.

[29] La *privacy by design* prevede che protezione dei dati sia implementata fin dalla progettazione del servizio, prodotto ecc. Al contrario, la *privacy by default* implica una tutela dei soggetti secondo un'impostazione predefinita.

[30] C. Bomprezzi, A. Gambino, *Come individuare il titolare del trattamento alla luce del Gdpr*, disponibile qui: https://www.agendadigitale.eu/sicurezza/privacy/gdpr-il-rapporto-tra-blockchain-e-titolare-del-trattamento/

[31] Ibid.

[32] The European Union Blockchain Observatory and Forum, *Blockchain and the GDPR report*, https://www.eublockchainforum.eu/

[33] Ipotesi di contitolarità del trattamento, come descritta dall'articolo 26 del GDPR.

[34] "Il presente regolamento non si applica ai trattamenti di dati personali: (a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; (b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE; (c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; (d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse".

[35] C. Bomprezzi, A. Gambino, Come individuare il titolare del trattamento alla luce del Gdpr, disponibile qui: https://www.agendadigitale.eu/sicurezza/privacy/gdpr-il-rapporto-tra-blockchain-e-titolare-del-trattamento/

[36] Articolo 5, comma 1, lettera a, GDPR.

[37] The European Union Blockchain Observatory and Forum, Blockchain and the GDPR report, https://www.eublockchainforum.eu/

[38] Articolo 5, comma 1, lettera c, GDPR.

[39] Articolo 5, comma 1, lettera d, GDPR

[40] M. Fink, *Blockchains and Data Protection in the European Union*, Max Planck Institute for innovation & Competition Research paper, n. 18-01, https://edpl.lexxion.eu/article/edpl/2018/1/6

[41] Articolo 16, GDPR.

[42] The European Union Blockchain Observatory and Forum, *Blockchain and the GDPR* report, https://www.eublockchainforum.eu/

[43] Articolo 17, GDPR.

[44] Articolo 17, comma 2, GDPR.

[45] M. Nicotra, *Blockchain e GDPR: le norme da conoscere per tutti i problemi*, disponibile qui: https://www.agendadigitale.eu/sicurezza/blockchain-e-gdpr-le-norme-da-conoscere-per-tutti-i-problemi/

[46] Può sapere se sia in corso un trattamento dei propri dati personali e quindi ottenere accesso ai tutte le informazioni, come specificatamente identificate dall'articolo in questione.

[47] Consultabile qui: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679

[48] Sono stringhe formate da numeri e lettere che consentono di identificare tramite pseudonimo un soggetto fisico o giuridico.

[49] *Il Data Protection Working Party*, costituito in base all'articolo 29 della Direttiva 1995/46/CE.

[50] M. Finck, *Blockchains and Data Protection in the European Union*, Max Planck Institute for innovation & Competition Research paper, n. 18-01, https://edpl.lexxion.eu/article/edpl/2018/1/6

[51] Ibid.

[52] Ibid.

[53] In questo senso quindi è auspicabile l'implementazione e lo sfruttamento di tecniche di offuscamento, crittografia, anonimizzazione e anche la raccolta dei dati off-chain.