ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

18 MAGGIO 2022

Blockchain e big data nel settore pubblico: spunti in tema di G.D.P.R. compliance

di Giovanni Gallone
Magistrato amministrativo presso il T.A.R. Puglia

Blockchain e big data nel settore pubblico: spunti in tema di G.D.P.R. compliance*

di Giovanni Gallone
Magistrato amministrativo presso il T.A.R. Puglia

Abstract [It]: L'applicazione della tecnologia *blockchain* al settore pubblico si intreccia inevitabilmente, anche nella prospettiva dell'automazione delle decisioni amministrative, con il tema della gestione e sfruttamento dei *big data* offrendo enormi potenzialità ma anche ponendo inediti problemi di compatibilità con la disciplina giuridica europea e nazionale in tema di data protection.

Title: Blockchain and big data in the Public Administration: some reflections on G.D.P.R. compliance
Abstract [En]: The application of *blockchain* technology to the public sector is inevitably linked, also from the perspective of the automation of administrative decisions, with the issue of the management and exploitation of *big data*, offering enormous potential but also posing unprecedented problems of compatibility with European and national legal regulations on data protection.

Parole chiave: Blockchain; Pubblica Amministrazione; Registro Distribuito; G.D.P.R.; Big Data
Keywords: Blockchain; Public Administration; Distributed Ledger; G.D.P.R.; Big Data

1. La tecnologia blockchain nella moderna società dei dati

I primi studi in tema di applicazione della *blockchain* al settore pubblico[1] si sono concentrati sulle potenzialità più evidenti di questa tecnologia, ponendo l'accento sull'impatto che questa è destinata ad avere sull'organizzazione e sull'azione amministrativa.

L'immodificabilità delle operazioni inserite nella catena di blocchi, la condivisione *ab origine* dei dati tra i partecipanti alla rete ed il passaggio dal tradizionale sistema a fiducia accentrata a forme di fiducia distribuita (con il conseguente mutamento di ruolo della Pubblica Amministrazione) rappresentano, però, solo le ricadute più immediate dei registri informatici distribuiti.

* Articolo sottoposto a referaggio.

1 M. ATZORI, *Blockchain technology and decentralised governance: is the State still necessary?*, in *Journal of governance and regulation*, 2017, 6(1), 45, G. GALLONE, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, in *Il diritto dell'economia*, 3, 2019 196, M. ALLENA, *Blockchain technology for environmental compliance: towards a choral approach*, in *Enviromental Law Review*, 4, 2020 e M. MACCHIA, *Blockchain e pubblica amministrazione*, in *Federalismi*, 2, 2021. Sul tema dei rapporti tra automazione contrattuale amministrativa e tecnologia blockchain cfr. anche G. GALLONE, *Public Administration and the Challenge of Contractual Automation. Notes on Smart Contracts*, in *European Review of Digital Administration & Law*, 1, 1-2, 2020, 179.

Le reali potenzialità di una tecnologia tanto dirompente e dal campo di applicazione così ampio possono, per contro, essere apprezzate nella loro pienezza solo se lette nel panorama complessivo e variegato della quarta rivoluzione industriale[2].

In questa prospettiva, la tecnologia blockchain si candida certamente a rivestire un ruolo di primo piano nella moderna società dei dati[3].

Se, infatti, i *big data* rappresentano, per importanza, il nuovo carburante dell'economia digitale[4], la sfida più delicata che si pone, non solo agli operatori economici ma anche ai decisori pubblici[5], è quella di rendere una così enorme mole di dati sempre più agevolmente sfruttabile. La depurazione dei dati rappresenta la tappa principale verso una transizione "green"[6] anche nel settore digitale, in grado di porre, in qualche maniera, rimedio alle storture del capitalismo della sorveglianza[7]. Agevolare la lettura in chiaro e trasparente dei mega dati è, infatti, il primo rimedio per avversare una gestione oscura (e concentrata nelle mani di poche imprese private) di una risorsa così importante e delicata[8].

Ma l'aspetto di maggiore interesse è, probabilmente, quello legato alla combinazione virtuosa che può scaturire tra registri distribuiti, lettura in chiaro dei *big data* ed automazione decisionale pubblica. Le capacità di elaborazione, ancora in massima parte da esplorare, dell'intelligenza artificiale[9], specie nelle forme del *machine learning*, escono, infatti, inevitabilmente esaltate dalla possibilità di disporre di un grande

2 K. SCHWAB, *The Fourth Industrial Revolution*, Penguin Books Ltd., Londra, 2015.

3 Tra i primi a riflettere sul tema E. KARAFILOSKI, A. MISHEV, *Blockchain Solutions for Big Data Challenges. A literature review*, in IEEE EUROCON 2017 - 17th International Conference on Smart Technologies, 2017, 763-768 e K. RABAH, *Convergence of AI, IoT, BigData and Blockchain: a review*, *The Lake Institute journal*, 2018, 1, 1 e ss..

4 "Data is the new oil. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc to create a valuable entity that drives profitable activity; so must data be broken down, analyzed for it to have value" secondo la famosa affermazione del matematico britannico Clive Humby.

5 Potenzialità ormai intuite da tempo: M. MACIEJEWSKI, *To do more, better, faster and more cheaply: using big data in public administration*, in *International Review of Administrative Sciences*, 2017, 120 e F. COSTANTINO, *Lampi. Nuove frontiere delle decisioni amministrative tra open e big data*, in *Dir. Amm.*, 2017, 4, 799. In Italia, per quanto riguarda il rapporto tra dati e funzioni amministrative si veda, in particolare, il lavoro di G. CARULLO, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, 2016, 21 e ss.

6 M. ATZORI, *Blockchain technology and decentralised governance: is the State still necessary?*, *cit.*, 51.

7 Nel quadro descritto da S. ZUBOFF, *The Age of Surveillance Capitalism. The fight for a human future and the new frontier of power*, Public Affairs, New York, 2019.

8 La detenzione dei dati al pari di tutte le altre forme di codifica del capitale (nella lettura trasversale offerta da K. PISTOR, *The Code of Capital: How the Law Creates Wealth and Inequality*, Princeton University Press, Princeton, 2019) è fattore di polarizzazione della ricchezza (J. STIGLITZ, *The price of inequality. How Today's Divided Society Endangers Our Future*, W. W. Norton & Company, New York, 2012). I risvolti più oscuri del fenomeno erano già stati preconizzati da V. MAYER-SCHONBERGER, K. CUKIER, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, Houghton Mifflin Harcourt, Boston, 2013 e C. O'NEILL, *Weapons of Math destruction*, Penguin Books Ltd., Londra, 2017. Il "lato oscuro della trasparenza" e le incognite che si celano dietro la dismissione di ogni diaframma rispetto alla conoscibilità del dato sono stati indagati, anche sul piano informatico, ad ampio spettro tra "*miti ed ombre*" da A. G. OROFINO, *La trasparenza oltre la crisi. Accesso, informatizzazione e controllo civico*, Bari, 2020, passim e 285 e ss..

9 D. MARONGIU, *L'intelligenza artificiale "istituzionale": limiti (attuali) e potenzialità*, in *European Review of Digital Administration & Law*, 1, 1-2, 2020, J. VALERO TORRIJOS, *The Legal Guarantees of Artificial Intelligence in Administrative Activity: Reflections and Contributions from the Viewpoint of Spanish Administrative Law and Good Administration Requirements*, in *European Review of Digital Administration & Law*, 1, 1-2, 2020, 55, C. FRAENKEL-HAEBERLE, F*ully Digitalized Administrative Procedures in the German Legal System*, in *European Review of Digital Administration & Law*, 1, 1-2, 2020, 105.

quantitativo di informazioni che, a mezzo della *blockchain*, sia tracciabile e di più facile consultazione. Questo apre al decisore pubblico nuove frontiere di complessità ed accuratezza nella ponderazione e valutazione degli interessi pubblici con evidenti riflessi sull'efficacia dell'azione amministrativa[10].

2. Le potenzialità dei registri distribuiti nella gestione e sfruttamento dei big data

Lo sviluppo delle tecnologie informatiche è stato accompagnato da un progressivo ed inarrestabile aumento dei dati prodotti dagli utenti. Secondo le stime più attendibili[11] nel solo 2020 sarebbero stati creati, raccolti, archiviati, copiati ed elaborati 59 zettabyte di dati. La cifra è ancor più impressionante e rende l'idea della crescita esponenziale di questa mole, se si considera che tra il 1984 ed il 2016 (nell'arco, quindi, di 32 anni totali) sulla rete internet ne sono transitati complessivamente meno di 5 zettabyte[12].

Questo trend di crescita è, con tutta probabilità, anche sulla spinta della transizione digitale, destinato ad essere confermato nei prossimi anni. L'aumento dei dati prodotti e potenzialmente disponibili spinge, peraltro, alla costruzione di data set di sempre maggiori dimensioni[13].

Ciò impone, specie in prospettiva futura, l'abbandono del modello tradizionale dell'*information silo*, inteso come l'archiviazione di dati fissi che rimangono sotto il controllo di un unico gestore isolati dal resto del sistema, per passare a forme di gestione degli stessi più innovative ed efficaci, esigenze, queste, solo in parte soddisfatte attraverso il *cloud computing*[14].

Infatti, il modello dei *data silos*, ancora largamente dominante almeno nelle Amministrazioni pubbliche, con la sua strutturazione piatta dovuta all'immagazzinamento progressivo per strati dei dati, pone problemi non solo di efficienza (in termini di velocità nel reperimento, accesso ed elaborazione dei dati) ma anche di coerenza complessiva atteso che quando sono presenti due o più silos per dati in tutto o in parte coincidenti, il loro contenuto potrebbe essere diverso, disallineato e, in quanto tale, fonte di

10 È la frontiera rappresentata dalla data *analysis automation* e dalla *augmented analytics*, con ciò intendendosi la capacità di utilizzare tecnologie come l'intelligenza artificiale, il *machine learning* e il linguaggio naturale per esplorare il dato e analizzare come il contenuto viene sviluppato, consumato e condiviso. Si pensi, ad esempio, alla possibilità di elaborare l'enorme quantità di dati gestita attraverso una blockchain amministrativa in materia sanitaria (numero di accessi, numero di pazienti, tipologia di patologie etc.) attraverso strumenti di intelligenza artificiale per stabilire la localizzazione più efficiente sul territorio di un ospedale.

11 Sono cifre tratte dal Global Dataphere della International Data Corporation (IDC) pubblicato l'8 maggio 2020.

12 Cisco Visual Networking Index, 2018.

13 Per data set si intende un insieme di dati strutturati in forma relazionale che possa, come tale, formare oggetto di analisi. La tendenza alla costruzione di data set di dimensioni sempre maggiori si spiega con la constatazione, quasi banale, che l'allargamento della base di dati oggetto di analisi contestuale consente l'estrazione di informazioni aggiuntive rispetto a quelle che si potrebbero ottenere analizzando piccole serie, con la stessa quantità totale di dati.

14 Il paradigma del *cloud computing* prevede il *Data as a Service* (in acronimo *DaaS*) ossia la messa a disposizione dell'utente via web dei dati come se gli stessi fossero fisicamente presenti sul disco locale.

potenziale entropia e di errori. Il *cloud computing*, che pure riduce questi inconvenienti, resta carente sotto il profilo dell'integrità e sicurezza[15].

È di tutta evidenza che queste soluzioni sono destinate a rivelarsi inadeguate specie se si pone mente al fatto che, ormai, le caratteristiche qualitative dei *big data* non sono più racchiuse nella formula delle "3 V" (Volume, Velocity e Variety)[16] ma sono espresse, più compiutamente, anche dai due ulteriori attributi della "Veracity" e del "Value". Più segnatamente, ad assumere primaria importanza sono, ormai, i profili della qualità del dato (in termini di affidabilità del *data content*) e della capacità di questo di trasformarsi, appunto, in valore aggiunto, attraverso la sua elaborazione.

È questo il passaggio che porta dai *big data* agli *smart data* ed in esso può giocare un ruolo cruciale la tecnologia *blockchain*[17].

La possibilità di contare su un registro distribuito ed immodificabile importa, infatti, una serie di indubitabili vantaggi tecnici nella gestione di grandi quantitativi di dati complessi. Anzitutto, l'applicazione della tecnologia *blockchain* al *data storage* consente di elevare notevolmente il livello di sicurezza complessiva, azzerando quasi del tutto il rischio di una manomissione delle informazioni che vi sono inserite (la cd. *data integrity*). Inoltre, la sua struttura distribuita consente di ridurre frequenza ed impatto degli episodi di malfunzionamento, rendendo, peraltro, più agevoli le eventuali operazioni di ripristino[18].

Sotto altro profilo, l'impiego della tecnologia *blockchain* permette di implementare la qualità dei dati. Molto spesso i dati acquisiti dall'esterno ed inseriti nel database, provenendo da fonti diverse, sono destrutturati e presentano spesso formati diversi. Il loro inserimento nel registro distribuito consente, invece, una loro prima strutturazione ed uniformazione. Questa conversione in un formato più strutturato incide inevitabilmente sulla capacità del dato di generare valore (il *Value* di cui si è detto) in quanto agevola ed

15 Il *cloud computing* resta particolarmente esposto, per sua natura, essendo i dati di regola immagazzinati presso soggetti terzi estranei, a episodi di *data breach*. La scelta del ricorso al cloud pone peraltro una serie di importanti spunti di riflessione in tema di sovranità digitale e cybersecurity messi in evidenza, quanto alla situazione italiana ed all'avvio dell'*hub* del progetto europeo Gaia X da L. BOLOGNINI, E. PELINO, *Le tentazioni del cloud europeo e nazionale: tra semplificazione politica e critica giuridica*, in *Istituto italiano per la privacy e la valorizzazione dei dati*, 25 settembre 2020 e M. RHAO, *Gaia X: un'analisi giuspubblicistica dei cloud europei*, in *Gruppo di Pisa*, 3, 2021, 283. Sulle novità introdotte nell'ambito del P.N.R.R. dal D.L. n. 77 del 2021 in tema di "cloudificazione" della pubblica amministrazione G. SGUEO, *La transizione digitale*, in *Giornale di Diritto Amministrativo*, 6, 2021, 746 e ss..

16 È il noto modello elaborato da D. LANEY, *3D Data Management: Controlling Data Volume, Velocity and Variety*, Gartner, 2001.

17 Sul punto il rinvio è, tra gli altri, per una aggiornata visione di insieme a N. DEEPA, QUOC-VIET PHAM, C. DINH NGUYEN, SWETA BHATTACHARYA, B. PRABADEVI, THIPPA REDDY GADEKALLU, PRAVEEN KUMAR REDDY MADDIKUNTA, FANG FANG, PUBUDU N. PATHIRANA, *Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions*, 2020.

18 In questo senso, la condivisione del registro da parte degli operatori rende praticamente superfluo il compimento di operazioni di *back up* posto che il recupero dei dati potrà avere luogo semplicemente attingendo a quanto in possesso di ciascun nodo (che detiene una propria copia, identica alle altre, del registro).

accelera le operazioni di *data mining*, anche nella prospettiva di un utilizzo delle informazioni in chiave predittiva attraverso strumenti di intelligenza artificiale[19].

In più il funzionamento della *blockchain*, che si fonda sulla registrazione sequenziale delle operazioni compiute con l'apposizione alle stesse di un marcatore temporale (*time stamp*), apre alla possibilità di operare una analisi in tempo reale dei dati, attraverso il continuo monitoraggio del loro flusso (il *Real Time Data Analytics*). Ciò si accompagna, con evidenti riflessi sul piano organizzativo, ad una semplificazione del ciclo di vita del dato, che diventa più lineare sia rispetto al suo trattamento (interamente tracciato) e che nell'accesso ad esso (essendo condiviso *ab origine* da parte di tutti i partecipanti alla rete)[20]. Questa semplificazione comporta, peraltro, intuibili vantaggi non solo sotto il profilo dell'efficienza ma anche in termini di costi e di risorse necessarie alla gestione dei *big data*.

3. I risvolti dell'applicazione della tecnologia blockchain al settore pubblico e le interferenze con il data protection

Gli enormi vantaggi insiti nell'impiego della tecnologia *blockchain* nella gestione dei *big data* sono ancora più evidenti se si guarda al settore amministrativo.

Quest'ultimo, infatti, per sua natura, è portato alla gestione di una grande e complessa mole di dati.

Il decisore pubblico, peraltro, continua ad avvertire ciò ancora come una responsabilità ed un peso più che come una risorsa strategica nello sviluppo delle proprie politiche. In questo atteggiamento di diffidenza gioca un ruolo fondamentale, oltre che la mentalità di apparato, l'evidente interferenza che vi è tra gestione (e sfruttamento) dei *big data* in possesso dell'Amministrazione e compiti e doveri di *data protection*[21].

19 N. DEEPA, QUOC-VIET PHAM, C. DINH NGUYEN, SWETA BHATTACHARYA, B. PRABADEVI, THIPPA REDDY GADEKALLU, PRAVEEN KUMAR REDDY MADDIKUNTA, FANG FANG, PUBUDU N. PATHIRANA, *Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions*, cit. 4.

20 La dottrina parla di "Streamlining the Data Access", in N. DEEPA, QUOC-VIET PHAM, C. DINH NGUYEN, SWETA BHATTACHARYA, B. PRABADEVI, THIPPA REDDY GADEKALLU, PRAVEEN KUMAR REDDY MADDIKUNTA, FANG FANG, PUBUDU N. PATHIRANA, *Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions*, *cit.* 5.

21 L'intero impianto della disciplina europea in materia di *data protection* (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati - *General data protection regulation* in acronimo G.D.P.R. reperibile su www.eur lex.europa.eu), si fonda, del resto, sul concetto di *accountability* del titolare del trattamento (così i considerando 13, 74 e 79 e art. 24 del Regolamento). Per una visione di insieme della nuova disciplina M.G. Stanzione*, Il regolamento europeo sulla privacy. Origini e ambito di applicazione*, *in Eur. Dir. Priv.*, 2016, 4, 1249 e ss., L. Bolognini, E. Pelino, Bistolfi, *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016 e G. Finocchiaro (a cura di)*, Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017. L'attuazione e recepimento del G.D.P.R. da parte delle Pubbliche Amministrazioni importa, poi, oneri organizzativi anche particolarmente gravosi tra cui l'individuazione di un *Data Protection Officer* (art. 37 del G.D.P.R.) e la predisposizione di un registro dei trattamenti (art. 30 del G.D.P.R.).

Non può, infatti, obliterarsi che i dati gestiti dalla Pubblica Amministrazione hanno, normalmente, carattere personale ex art. 4 n. 1) del G.D.P.R.[22].

L'applicazione della tecnologia *blockchain* alla gestione dei dati in possesso dell'Amministrazione apre, peraltro, uno scenario totalmente inedito[23].

È, infatti, ormai opinione diffusa che la tecnologia della *blockchain* sia destinata ad avere un impatto significativo sulla scienza dell'amministrazione, mettendo in discussione i modelli e le categorie tradizionali[24]. Per quanto qui di interesse, la sua applicazione spinge a ritenere parzialmente superata anche l'idea stessa di trasparenza. Con la scomparsa di un'autorità centrale detentrice dei documenti e delle informazioni (che sono, invece, condivise tra tutti i partecipanti al database distribuito) alla accessibilità e visibilità dall'esterno si sostituisce, in chiave di coinvolgimento attivo, la condivisione *ab origine* dei dati. Essi nascono condivisi e dalla loro condivisione traggono, peraltro, l'attributo dell'immodificabilità.

L'accessibilità totale ed immediata al dato assicurata ai partecipanti dal registro distribuito sembra, all'apparenza, in frontale contrasto con la tutela della riservatezza dei titolari degli stessi. Delle possibili tensioni tra *blockchain* e G.D.P.R. si sono, peraltro, immediatamente avvedute tanto la dottrina[25] quanto le stesse istituzioni europee[26].

I dati annotati nel registro *blockchain*, oltre ad essere fisiologicamente pubblici e potenzialmente conoscibili da chiunque, sono immodificabili e ciò può stridere con la realizzazione del principio di minimizzazione

22 E tra questi anche dati "genetici", "biometrici" e "relativi alla salute" ex art. 4 nr. 13), 14) e 15) del G.D.P.R.. Il tema del trattamento dei dati sensibili da parte dell'amministrazione attraverso strumenti informatici è stato oggetto di interessanti riflessioni anche prima dell'avvento del G.D.P.R. fuori dei confini italiani (J. VALERO TORRIJOS, *Las transformaciones de la innovación tecnológica en la administración pública y su proyección sobre la protección de los datos de caractér personal*, in *La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, 56, 2012 e C. SARMIENTO E CASTRO, *Direito da informática, privacidade e dados pessoais*, Coimbra, 2003, 170 e ss.).

23 Sono considerazioni in parte già svolte in G. GALLONE, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, *cit.*, 196.

24 In proposito, si vedano le riflessioni di M. A. BERNAL BLAY, *Blockchain, Administración y contratación pública*,in *Observatorio de Contratación Pública*, 12 luglio 2018, B. BARRAUD, *Les blockchains et le droit*, in *Reveu Lamy droit de l'immateériel*, 147, 2018, 48 e M. Macchia*, Blockchain e pubblica amministrazione*, *cit.*.

25 Sul tema dei rapporti tra questa disciplina e la tecnologia blockchain cfr. M. BERBERICH, M. STEINER, *Practitioner's Corner. Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?*, in *European Data Protection Law Review*, 3, 2016, M. FINCK, *Blockchains and Data Protection in the European Union*, in *Max Planck Institute for innovation & Competition Research paper*, 18-01, 30 novembre 2017, L. IBANEZ, K. O'HARA, E. SEMPERL, *On blockchains and the general data protection regulation*, *EU Blockchain Forum and observatory*, 7,2018, A. M. GAMBINO, C. BOMPRESSI*, Blockchain e protezione dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 3, 2019, A. PALLADINO, *L'equilibrio perduto della blockchain tra platform revolution e GDPR compliance*, in *Rivista di diritto dei media*, 2/2019 e A. GIANNOPOULOU, *Putting privacy by design on the blockchain*, in *European Data Protection Law Review*, 2021, 388 - 399.

26 Cfr. Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772(RSP)) che muove dall'idea che la tecnologia dei registri distribuiti prevede "la pseudonimizzazione degli utenti, ma non la loro anonimizzazione" (Considerando D) per concludere nel senso della piena sottoposizione della stessa alla disciplina del G.D.P.R.. Sul punto cfr. anche il report tematico *Blockchain and the GDPR*, a cura dello European Union Blockchain Observatory, 16 ottobre 2018, pubblicato su www.eublockchainforum.eu.

dei dati ex art. 5 G.D.P.R. e, in particolare, con la definizione di tempi limitati di conservazione degli stessi[27].

Sul piano organizzativo, la codetenzione del dato da parte di tutti i partecipanti alla *blockchain* impone, poi, di ripensare le soluzioni più rodate in tema di individuazione dei soggetti titolari e responsabili del trattamento.

Si pone, così, in tutta la sua complessità, il problema della *G.D.P.R. compliance*, aspetto qualificante della *blockchain governance*[28] in relazione alla quale emerge la perdurante indispensabilità di un attore pubblico che preveda una disciplina di funzionamento del network che sia conforme, sul piano tecnico e giuridico, al diritto positivo interno ed europeo[29].

4. Blockchain amministrativa e G.D.P.R.

La difficolta di fondo nel conciliare le caratteristiche della tecnologia *blockchain* con la disciplina europea è rappresentata dalla circostanza che il G.D.P.R., pur riferendosi espressamente anche al trattamento dei dati personali ad opera delle "autorità pubbliche"[30] è modellato sulle forme tradizionali di trattamento centralizzato attraverso i *data silos*.

In assenza di una disciplina normativa *ad hoc*, per distendere le possibili tensioni tra *blockchain* amministrativa e G.D.P.R. occorre, quindi, prendere le mosse dall'assetto che il registro distribuito può concretamente assumere.

27 A. PALLADINO, *L'equilibrio perduto della blockchain tra platform revolution e GDPR compliance*, *cit*., 153. È quanto stabilito all'art. 5 par. 1 lett. c) ed e) del G.D.P.R. in base al quale i dati devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" e "devono essere conservati in modo da consentire l'identificazione degli interessati per un tempo non superiore a quello necessario al conseguimento della finalità del trattamento".

28 Nell'ecosistema blockchain il ruolo dell'Amministrazione non è più quello di motore unico del rapporto, ma di garante delle regole del sistema e si risolve, pertanto, non solo nella "*governance by blockchain*" e, cioè, nel governare attraverso detto strumento, ma si sostanzia soprattutto nella "*blockchain governa*nce" ovvero nel governo dello strumento stesso (riprendendo le riflessioni di S. ØLNES, J. UBACHT, M. JANSSEN, *Blockchain in government: benefits and implications of distributed ledger technology for information sharing*, in *Government information quarterly*, 2017).

29 Non può, del resto, sfuggire, quanto all'Italia, che è lo stesso art. 50 comma 1 del D.Lgs. n. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) a stabilire che "I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico".

30 Come noto, i nr. 7), 8), 9) e 10) recanti la definizione di "titolare del trattamento", di "responsabile del trattamento", di "destinatario" e di "terzo" vi ricomprendono anche "l'Autorità pubblica". Inoltre, l'art. 6 par. 1 lett e) contempla come condizione di liceità del trattamento dei dati personali, accanto al consenso dell'interessato, anche "l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".

Il dibattito sulla scelta tra il modello della *blockchain permissonless* (o pubblica) e *permissioned* (o privata)[31] si colora spesso di tinte quasi ideologiche tanto da spingere i puristi ad affermare che il secondo si collochi addirittura fuori dal paradigma della tecnologia, quasi ne costituisse un tradimento.

Eppure, sembra che, quantomeno nel prossimo futuro, l'unica alternativa effettivamente praticabile per lo sfruttamento della tecnologia *blockchain* nel settore pubblico sia costituita dal modello *permissioned*[32].

Quest'ultimo, oltre ad esprimere una migliore performance tecnica e a non soffrire della volatilità proprie delle reti aperte, consente di meglio fronteggiare (e superare) le criticità sopra descritte in tema di *data protection*.

Solo l'opzione per il modello *permissioned* permette, infatti, di rispondere ai canoni fondamentali della *privacy by design* e della *privacy by default* sanciti dall'art. 25 del G.D.P.R.. In base ad essi l'architettura del registro distribuito deve consentire, sin dal momento della sua progettazione e per sua impostazione predefinita, una protezione dei dati personali conforme agli standard del Regolamento. Ne consegue che il problema della *G.D.P.R. compliance* deve essere affrontato e risolto *ex ante* attraverso l'adozione di misure di natura tecnica e organizzativa. Peraltro, i principi in parola non hanno carattere assoluto e rigido ma, per espressa previsione del G.D.P.R., flessibile sicché il giudizio di adeguatezza e di esigibilità delle suddette misure di protezione deve essere condotto in concreto anche sulla base di una analisi costi-benefici[33]. Ne consegue che il decisore pubblico, in sede di *governance* della *blockchain*, conserva un margine di apprezzamento abbastanza largo, che consente di vagliare soluzioni diverse in grado di conciliare protezione dei dati personali e potenzialità dei registri distribuiti, rispetto del G.D.P.R. ed efficienza dell'azione amministrativa.

Sono diversi gli accorgimenti tecnici e organizzativi suggeriti in dottrina che permettono di scongiurare quello che è stato definito il paradosso di una *blockchain permissioned* esentata dal rispetto del G.D.P.R.[34].

---

31 Nella *blockchain permissionless*, alla base dell'esperienza del Bitcoin, l'accesso al network è totalmente libero ed il controllo è distribuito ed affidato a tutti i partecipanti. Nel modello della *blockchain permissioned*, invece, tanto l'accesso quanto l'attività di validazione è riservata ad un gruppo ristretto di partecipanti.

32 G. GALLONE, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, *cit*., 197.

33 Stabilisce, in proposito, l'art. 25 del G.D.P.R. che le misure di protezione devono essere definite "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento". Si tratta di una declinazione specifica del tema della gestione dei rischi (in questo caso collegati al trattamento di dati personali) insiti nello svolgimento dell'attività amministrativa sui quali si rinvia, tra tutti, all'impostazione di A. BARONE, *Il diritto del rischio*, Milano, 2006 ripresa e dettagliata dallo stesso Autore in *Amministrazione del rischio e intelligenza artificiale*, in *European Review of Digital Administration & Law*, , 1, 1-2, 2020, 63. In linea con i dettami del risk management il Regolamento recepisce, peraltro, una nozione del rischio non limitata alla fase della violazione, ma anche a quella precedente in cui la violazione non ha ancora avuto luogo (A. M. GAMBINO, C. BOMPRESSI*, Blockchain e protezione dei dati personali*, *cit*., 621).

34 A. MIRCHANDANI, *The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR*, in *Fordham Intellectual Property*, *Media and Entertainment Law Journal*, 4, 2019.

Sul piano organizzativo, se nelle *blockchain permissionless* si riscontra un evidente difetto di *accountability* nella trattazione dei dati, in quelle *permissioned* è, invece, possibile individuare preventivamente, all'atto della fissazione della disciplina di funzionamento della rete, il nodo (o i nodi) titolari o responsabili del trattamento.

È stato, in proposito, condivisibilmente osservato[35] come sia lo stesso art. 26 del G.D.P.R. ad ammettere forme di contitolarità del trattamento. Ciò sembrerebbe consentire, calando la previsione in parola nel contesto proprio della *blockchain* (caratterizzata dalla condivisone *ab origine* dei dati da parte di tutti gli operatori), il riconoscimento della qualità di titolare del trattamento a tutti i partecipanti alla rete. Tuttavia, ciò si tradurrebbe in una ingiustificata moltiplicazione degli adempimenti amministrativi relativi al trattamento dei dati personali (che ricadrebbero in larga misura anche su soggetti privati) con conseguente complessivo appesantimento dell'azione amministrativa. Inoltre, l'individuazione di un numero potenzialmente elevato di contitolari del trattamento rischia di generare pericolose interferenze nello svolgimento delle funzioni collegate a tale qualità.

Sotto il profilo squisitamente giuridico va, poi, evidenziato che si ha contitolarità del trattamento solo ove "due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento"[36]. In questo senso sembra che la mera partecipazione alla rete ed il riconoscimento del potere di validazione delle operazioni compiute non sia sufficiente ad attribuire la contitolarità del trattamento richiedendo ciò un *quid pluris* consistente nel potere di stabilire scopo e *quomodo* del trattamento stesso.

In una *blockchain* amministrativa questo ruolo di definizione di "finalità" e "mezzi" del trattamento dovrà spettare ragionevolmente al nodo "pubblico" o "amministrativo" (id est la pubblica amministrazione che ha allestito la rete e che si occupa della sua *governance*). Questo nodo "amministrativo" si ritaglia così un ruolo differenziato rispetto gli altri nodi "non amministrativi" che, invece, pur condividendo *ab origine* tutti i dati inseriti nel registro, non rivestiranno la qualità di titolare del trattamento[37].

Siffatta soluzione ha l'indubbio merito di ridurre la complessità soggettiva del sistema di protezione dei dati personali e di garantirne la maggiore efficienza. Del resto, una differenziazione, sotto il profilo giuridico, della posizione del nodo "amministrativo" rispetto a quella degli altri nodi "non amministrativi", pare comunque imposta dalla necessità di assicurare la conformità dello strumento alla

35 A. PALLADINO, *L'equilibrio perduto della blockchain tra platform revolution e GDPR compliance*, cit., 154.

36 Così art. 26 par. 1 G.D.P.R.. Questa nozione costituisce, a ben vedere, il riflesso di quella, più generale di "titolare del trattamento" posta dal n. 7) dell'art. 4 del G.D.P.R. Secondo cui è "titolare del trattamento […] la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".

37 M. FINCK, *Blockchains and Data Protection in the European Union*, *cit.*, 26 il quale, peraltro, osserva, con riferimento al testo dell'art. 4 nr. 7) del G.D.P.R. che "The use of the singular indicates that in centralised data silos there is often only one entity that qualifies as a data controller. It is to them that the GDPR is addressed".

disciplina interna ed eurounitaria in materia di identificazione elettronica di cui al il Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 (il c.d. «Regolamento eIDAS»), attraverso la previsione nella propria architettura di un *master node* che operi come soggetto erogatore della soluzione di firma elettronica attestando l'identità dei titolari delle chiavi crittografiche ammessi al network[38].

Inoltre, occorre tenere presente che la titolarità del trattamento è concetto ben diverso dalla responsabilità dello stesso. L'art. 4 nr. 7) e 8) del G.D.P.R. tengono, infatti, distinte la già esaminata nozione di "titolare del trattamento" da quella di "responsabile del trattamento" che si identifica con "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento[39]".

Non è, quindi, da escludere che in una *blockchain* amministrativa più complessa si possano prevedere una pluralità di nodi "a ruolo differenziato", contemplando, accanto ad un master node "amministrativo" che assommi in sé il ruolo di soggetto erogatore della soluzione di firma elettronica e di titolare del trattamento dei dati personali, uno o più nodi ulteriori anch'essi "amministrativi" che possano elaborare i dati in qualità di responsabili del trattamento[39].

Del resto, in uno scenario che vede la costruzione di network di dimensioni ridotte, con un numero contenuto di nodi, organizzati in forma *permissioned* e sottoposti a regolamentazione pubblica[40], in attesa della creazione di una dorsale pubblica unica fondata su registri distribuiti, si pone, sempre sul piano organizzativo, la questione della *G.D.P.R. compliance* rispetto al flusso di dati che normalmente avviene tra Pubbliche Amministrazioni[41] e, in particolare, tra *blockchain* amministrative in cui il ruolo di titolare del

38 Come già messo in evidenza in G. GALLONE, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, *cit.*, 197 e F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, Miano, 2018, 66.

39Ciò che assume importanza è che, in sede di definizione della disciplina di funzionamento della blockchain amministrativa, sia assicurata, come esige il Considerando 79 al G.D.P.R., "una chiara ripartizione delle responsabilità […] compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento".

40 Come quello immaginato da M. ATZORI, *Blockchain governance and the role of trust service providers: the trusted chain network*, Londra, 2017, 13 che immagina la tecnologia blockchain come inserita in un "multi-stakeholder framework" che assicuri un "appropriate mix of centralization and decentralization" ritagliato sulle esigenze concrete dei singoli processi. Sul tema B. VAN ALSENOY, *Allocating Responsibility among Controllers, Processors, and "Everything in between": The Definition of Actors and Roles in Directive 95/46/EC*, in *Computer Law & Security Review*, 25, 2012, 32.

41 Fenomeno che è espressamente ammesso, quanto all'ordinamento italiano, dal nuovo comma 2 art. 50 del D.Lgs. n. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale), come da ultimo modificato dall'art. 264, comma 2, lettera b), legge n. 77 del 2020, secondo cui "Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all'articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241, e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, salvo per la prestazione di elaborazioni aggiuntive". Il quadro è completato dal successivo comma 2 bis che stabilisce che Le pubbliche amministrazioni, nell'ambito delle proprie funzioni istituzionali, procedono all'analisi dei propri dati anche in combinazione con quelli detenuti da altri soggetti di cui all'articolo 2, comma 2, fermi restando i limiti di cui al comma 1. La predetta attività si svolge secondo le modalità individuate dall'AgID con le Linee guida".

trattamento dei dati personali compete a soggetti amministrativi differenti. Essa risulta legata al tema tecnico della interoperabilità[42] tra i diversi circuiti *blockchain* amministrativi e dipende, essenzialmente, dalla capacità della tecnologia di garantire che i dati migrati da un registro distribuito all'altro conservino gli attributi di immodificabilità e certezza temporale. La reciproca affidabilità delle piattaforme *blockchain*, consentendo l'integrale tracciabilità della vita del dato, ridimensionerebbe, infatti, notevolmente il problema di stabilire il momento in cui questo passa dalla disponibilità giuridica (e dalla responsabilità) di un titolare a quella dell'altro e se e, soprattutto, in quale frangente del trattamento si siano verificate violazioni della disciplina di legge.

Sul piano delle modalità di trattamento dei dati personali, anche con riguardo alla *blockchain* amministrativa, si pone il problema della tutela della riservatezza degli interessati. Il dato personale, infatti, non appena inserito nel registro distribuito diviene conoscibile (ed è addirittura codetenuto) da tutti i partecipanti al network. Ciò non impedisce, tuttavia, in sede di fissazione della disciplina di funzionamento della *blockchain permissioned*, di individuare talune categorie di dati destinanti a rimanere (temporaneamente o in perpetuo) riservati[43].

Del resto, è lo stesso G.D.P.R. a prevedere la possibilità di una "pseudonimizzazione"[44] dei dati. Dal punto di vista tecnico ciò può essere conseguito attraverso diverse soluzioni quali, ad esempio, l'impiego di firme cd. "ad anello"[45], multiple apposte da più operatori, così da non rendere il dato univocamente riconducibile ad uno di essi ovvero quello di aggregare grandi quantità di dati provenienti da diversi soggetti in un unico blocco con l'apposizione di una singola firma digitale[46].

È evidente che siffatte soluzioni consentono di celare la provenienza del dato ma non il contenuto in sé dello stesso. Tuttavia, ciò, escludendo la certa attribuibilità del dato a un interessato specifico in assenza

---

42 Sul tema della interoperabilità dei dati anche nell'ottica delle relazioni interorganiche si rinvia a G. CARULLO, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, cit., 129 e ss..

43Attraverso l'apposizione di una "limitazione di trattamento", definita dall'art. 4 par. 1 n. 3) del G.D.P.R. come un "contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro". L'esigenza di mantenere la riservatezza circa il contenuto di taluni blocchi della catena è particolarmente avvertita nel campo delle procedure di affidamento dei contratti pubblici rispetto alle offerte presentate dai partecipanti (che dovranno rimanere riservate fino, almeno, alla loro valutazione da parte della Commissione).

44 Art. 4 n. 5) del G.D.P.R. che definisce la "pseudonimizzazione" come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

45 È un tipo di firma digitale che costituisce l'evoluzione delle firme digitali di gruppo (categoria elaborata per la prima volta da D. CHAUM, E. VAN HEYST, *Group signatures*, in *Advances in Cryptology - Eurocrypt' 91*, 257 - 265, Berlino, 1991). Essa consente ad un qualsiasi membro di un gruppo predefinito di utenti di firmare messaggi in modo anonimo per conto del gruppo con la possibilità che un utente designato del gruppo possa successivamente revocare l'anonimato e identificare l'autore di una firma.

46 Sono le soluzioni tecniche suggerite nel *report* tematico *Blockchain and the GDPR*, a cura dello *European Union Blockchain Observatory*, *op. cit.*, 17 e ss..

di ulteriori specifiche informazioni[47], pare sufficiente, sul piano giuridico, alla luce della nozione di "pseudonimizzazione" impiegata all'art. 4 n. 5) del G.D.P.R., a garantire la piena *compliance* alla disciplina europea[48].

Le medesime tecniche di pseudonimizzazione possono, poi, rappresentare una soluzione anche per i diversi, benché connessi, problemi della "minimizzazione", della "limitazione della conservazione" dei dati e, di riflesso, della tutela del "diritto all'oblio" degli interessati[49].

Secondo la disciplina del G.D.P.R., una volta soddisfatta la finalità per la quale è disposto il trattamento, i dati dovrebbero essere cancellati. Ciò non è, tuttavia, possibile in un registro distribuito ove le operazioni compiute sono immodificabili (e non possono, quindi, essere espunte dalla sequenza).

Un'alternativa tecnicamente equipollente alla cancellazione può essere, tuttavia, rappresentata dalla anonimizzazione successiva, definitiva ed irreversibile del dato. Questo risultato può essere ottenuto, ad esempio, attraverso la distruzione delle chiavi di crittografia impiegate nel corso delle operazioni di pseudonimizzazione[50]. Meno soddisfacente è, invece, la soluzione dello stoccaggio fuori catena del dato da cancellare (*off chain storage*) che si limita a spostare fuori dell'ecosistema *blockchain* (e, quindi, fuori delle garanzie di verifica che lo stesso offre e con un aumento dei costi di gestione) l'operazione di distruzione. Peraltro, il tema della limitazione della conservazione dei dati nelle *blockchain* amministrative appare notevolmente ridimensionato dalla previsione dello stesso art. 5 par. 1 lett. e) del G.D.P.R.. Quest'ultima previsione contempla, infatti, nella sua seconda parte, un temperamento al principio generale stabilendo che i "dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative

47 Infatti, conoscendo la chiave pubblica (che funge da account) di un nodo diventa possibile ricollegare l'indirizzo ad una specifica identità, attribuendo così la paternità del dato.

48 È opinione condivisa dal Gruppo di lavoro istituito in virtù dell'articolo 29 della direttiva 95/46/CE nel Parere 05/2014 - WP 216 sulle tecniche di anonimizzazione adottato il 10 aprile 2014.

49 Art. 17 G.D.P.R. anche definito come "diritto alla cancellazione", che individua le ipotesi in cui "L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali", tra le quali rientra anche quella in cui i "dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati" e quella in cui "i dati personali sono stati trattati illecitamente". In dottrina sull'origine del diritto e sulla sua collocazione sistematica anche in prospettiva comparatistica cfr. J. AUSLOOS, *The Right to Erasure in EU Data Protection Law: From Individual Rights to Effective Protection*, Oxford, Oxford University Press, 2020, M. MEZZANOTTE, *Il diritto all'oblio*, Edizioni Scientifiche Italiane, Napoli, 2009. Quanto al diritto all'oblio nel G.D.P.R. cfr. A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018*, n. 101, Zanichelli, Bologna, 2019, 392 e G. RUGANI, *Il diritto all'oblio dell'art. 17 del Regolamento (UE) 2016/679: una grande novità? Una denominazione opportuna*, in A. MANTELERO, D. POLETTI, *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei sati personali. Un dialogo tra Italia e Spagna*, Pisa University Press, Pisa, 2018, 455.

50 Tale soluzione richiede, peraltro, l'individuazione del nodo incaricato delle operazioni di distruzione delle chiavi di crittografia. Esso, può, tuttavia, coincidere, nella *permissioned blockchain*, con il master node "amministrativo" già designato come erogatore della soluzione di firma elettronica.

adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato". L' archiviazione nel pubblico interesse rappresenta, invero, un'ulteriore e peculiare forma di trattamento lecito dei dati personali differente da quella di base svolta in forza di una delle condizioni poste dall'art. 6 del G.D.P.R.[51]. La possibilità di archiviazione consente, anzitutto, di postergare la cancellazione del dato rispetto alla soddisfazione della finalità per la quale è disposto il trattamento. Inoltre, consente ex art. 17 par. 3 del G.D.P.R., addirittura di escludere il diritto alla cancellazione dell'interessato ove l'esercizio dello stesso "rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento" di archiviazione.

L'archiviazione di dati personali a mezzo di registro distribuito nel pubblico interesse è, del resto, aspetto cruciale nella costruzione di un *data set* ampio, che assuma i caratteri del *big data*, da cui attingere, anche attraverso l'impiego di strumenti di A.I., per l'adozione in forma automatizzata di decisioni amministrative.

Rimane, in ultimo, da chiarire come si possa garantire, anche in una *blockchain* amministrativa, il diritto degli interessati alla rettifica o integrazione ex art. 16 del G.D.P.R., dei dati personali inseriti nel registro distribuito, per loro natura immodificabili. Una parte della dottrina suggerisce, a soluzione di un problema che è eminentemente tecnico, il ricorso a *chameleon hash* che permettono di mantenere inalterato l'hash di sequenza pur effettuando cambiamenti nel singolo blocco[52]. In particolare, la *chameleon hash* altro non è che è una funzione hash crittografica che prevede una *backdoor* (un metodo, ignoto agli operatori, per aggirare il sistema crittografico) la cui chiave è nella disponibilità di uno solo dei nodi. È intuibile che nelle *permissioned blockchain* la chiave di *backdoor* andrà preferibilmente affidata al master node "amministrativo", già designato, come detto, quale erogatore della soluzione di firma elettronica.

La possibilità per il nodo "amministrativo" di rettificare il dato intervenendo sul contenuto del blocco sembrerebbe, peraltro, incrinare il carattere di immodificabilità proprio del registro distribuito mettendo a rischio la *data integrity*. Una simile preoccupazione è, tuttavia, infondata, E, infatti, ogni operazione, compresa quella di modifica, resta tracciata, non potendo il relativo blocco essere eliminato dalla catena in cui è inserito. In altri termini, l'operato del nodo detentore della chiave di *backdoor* resta monitorabile, secondo la logica di trasparenza che impronta la *blockchain*, dagli altri partecipanti, i quali potranno chiedere conto al nodo amministrativo di come questi ha fatto uso dello strumento (il c.d. *key management*,

51 Cfr. considerando 50. Sicché è certamente ipotizzabile un trattamento lecito in forma di archiviazione di dati personali già trattati "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" ex art. 6 par. 1 lett e) del G.D.P.R..

52 K. ASHRITHA, M. SINDHU AND K. V. LAKSHMY, *Redactable Blockchain using Enhanced Chameleon Hash Function*, in *5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, 2019, 323, M. FINCK, *Blockchains and Data Protection in the European Union*, *cit.*, 23 e A. M. GAMBINO, C. BOMPRESSI, *Blockchain e protezione dei dati personali*, *cit.*, 642.

parte del nuovo ruolo di *governance* dell'infrastruttura spettante alla Pubblica Amministrazione) chiamandolo a giustificare (e a rispondere) di ogni alterazione della sequenza.

5. Oltre le criticità: uno scenario in evoluzione

Se la tecnica offre, dunque, soluzioni tutto sommato agevoli per superare le criticità che si pongono nella costruzione di una *blockchain* amministrativa rispettosa della disciplina europea e nazionale in tema di protezione dei dati personali, non va trascurato come la tecnologia dei registri distribuiti sia, addirittura, in grado di elevare, sotto taluni aspetti, lo standard minimo di tutela posto dal G.D.P.R.[53].

Ciò è particolarmente evidente sul piano del coinvolgimento dell'interessato nel ciclo di vita del dato. In questo senso, la struttura multipolare della *blockchain* può consentire al singolo partecipante, all'atto dell'ammissione alla *blockchain permissioned*, di stabilire (attraverso un'operazione che è inserita al pari delle altre inserite nel registro distribuito) quali dati fornire e di modulare il consenso prestato al loro trattamento ma, soprattutto, di monitorare direttamente il trattamento stesso[54]. Questo accorgimento agevola il responsabile del trattamento nel censimento delle volontà degli interessati e rappresenta una tra le forme più interessanti ed innovative di cogestione del procedimento amministrativo[55].

Non va, poi, dimenticato, che l'impiego della tecnologia *blockchain* nell'ambito del settore pubblico per la gestione dei *big data* agevola e semplifica, sotto vari aspetti, i compiti del titolare del trattamento. In particolare, la trasparenza delle operazioni e la codetenzione del dato *ab origine* da parte di tutti gli operatori, pur con gli accorgimenti già visti in punto di tutela della privacy, produce un effetto di semplificazione delle procedure di gestione del dato diverse dal trattamento *stricto sensu*. Il diritto di accesso dell'interessato, nella sua duplice dimensione di diritto ad ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e di averne una copia[56], trova soddisfazione in via automatica, senza l'attivazione di uno specifico procedimento. Questa semplificazione elimina la necessità che l'interessato formuli un'istanza e che il titolare del trattamento la

53 Come è obiettivo dello stesso G.D.P.R. che al considerando n. 6 si prefigge, in chiave dinamica, di assicurare un "elevato livello di protezione dei dati personali".

54 G. ZYSKIND, O. NATHAN, A. PENTLAND, *Decentralizing privacy: using blockchain to protect personal data, Security and privacy workshops (SPW)*, 2015 IEEE, 2015 secondo cui attraverso il registro distribuito «users should own and control their data» e «are always aware of the data that is being collected about them and how it is used».

55 E' la prospettiva indagata da L. EDWARDS, M. FLINCK, M. VEALE, N. ZINGALES, *Data subjects as data controllers: a Fashion(able) concept?*, in *Internet Policy Review*, 2019.

56 Art. 15 G.D.P.R.. La codetenzione *ab origine* del dato può, al contempo, soddisfare, attraverso l'adozione di accorgimenti tecnici che consentano la lettura in chiaro della sequenza, anche il diritto alla portabilità dei dati ex art. 20 G.D.P.R. secondo cui "L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento".

riceva, la esamini e decida se accoglierla ostendendo o meno il dato. E tutto ciò si traduce chiaramente in un notevole risparmio di risorse umane ed economiche per la Pubblica Amministrazione[57].

A fronte di potenzialità così evidenti, lo scenario tecnico e regolatorio in materia di *blockchain* amministrative è, naturalmente, in evoluzione.

L'Italia si è collocata all'avanguardia in Europa sul piano normativo introducendo, al comma 1 dell'art. 8 ter del D.L. n. 135 del 2018[58], una definizione legale di "registro distribuito".

Questa novella normativa ha assunto una valenza essenzialmente descrittiva non essendo stata accompagnata dalla previsione di una disciplina di dettaglio[59]. Questo silenzio del legislatore è, tuttavia, probabilmente, da leggere come una lacuna intenzionale, frutto di una specifica scelta regolatoria ispirata al principio di neutralità tecnologica[60].

Peraltro, se, con quanto detto in precedenza, si è tentato di dimostrare che, anche a legislazione invariata, vi è la possibilità di costruire una *blockchain* amministrativa conforme alla disciplina europea (e di riflesso interna) in tema di protezione dei dati personali, sembra che permangano margini significativi per un intervento del legislatore nazionale per la definizione di una disciplina specifica.

---

[57] Semplificando notevolmente la "filiera dei dati" e lo svolgimento della funzione amministrativa per l'organizzazione e la gestione degli stessi (come ricostruita in G. CARULLO, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, cit., 81 e ss.).

58 Il riferimento è al decreto legge 14 dicembre 2018, n. 135, convertito con modificazioni con la legge 11 febbraio 2019, n. 12 di "Conversione in legge del decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione", pubblicata in G.U. n. 36 del l'11 febbraio 2019 secondo cui "Si definiscono «tecnologie basate su registri distribuiti» 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 crittografia verificabili da ciascun partecipante, non alterabili e non modificabili".

[59] Il comma 4 dell'art. 8 ter si limita, peraltro, a demandare all'Agenzia per l'Italia Digitale l'individuazione degli "standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3" e , quindi, solo quelli relativi alla "validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014" (il cd. timestamping) delle transizioni elettroniche, lasciando fuori da tale delega regolatoria ogni altro aspetto disciplinatorio della tecnologia.

Più di recente il Decreto Presidenza del Consiglio dei Ministri Dipartimento della Funzione Pubblica 12 agosto 2021 n. 148 "Regolamento recante modalità di digitalizzazione delle procedure dei contratti pubblici, da adottare ai sensi dell'articolo 44 del decreto legislativo 18 aprile 2016, n. 50", pubblicato sulla G.U. Serie Generale n. 256 del 26 ottobre 2021, ha espressamente fatto richiamo, nel campo dell'e-procurement, allo strumento della blockchain stabilendo, all'art. 9 comma 1, che "Il sistema telematico assicura agli utenti autenticati di cui all'articolo 3, la disponibilità dei dati e dei documenti gestiti, la cui integrità e segretezza è garantita anche attraverso l'uso di idonee tecniche di crittografia e offuscamento, mantenendo anche la tracciabilità degli accessi secondo quanto previsto dall'articolo 6 e garantendo la terzietà del gestore del sistema telematico anche mediante l'impiego di tecnologie basate su registri distribuiti, come definite dall'articolo 8-ter, comma 1, del decreto-legge 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla legge 11 febbraio 2019, n. 12".

[60] Su di esso cfr. A.G. OROFINO, *L'esternazione informatica degli atti amministrativi, in A 150 anni dall'unificazione amministrativa italiana - Studi*, a cura di L. FERRARA, D. SORACE, vol. IV*, La tecnificazione*, a cura di S. CIVITARESE MATTEUCCI e L. TORCHIA, Firenze University Press, Firenze, 2016, 181 e ss. Il principio di neutralità tecnologica come criterio guida nell'approccio alla tecnologia blockchain è suggerito anche dalla Risoluzione del Parlamento Europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione, *cit.*, considerando E.

In particolare, l'art. 6 par. 3 del G.D.P.R. prevede, per l'ipotesi in cui la base giuridica del trattamento dei dati personali sia l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, la possibilità per il diritto dello Stato membro cui è soggetto il titolare del trattamento (oltre che per il diritto dell'Unione) di introdurre, nel rispetto del principio di proporzionalità, "disposizioni specifiche per adeguare l'applicazione delle norme" del Regolamento con riguardo alle "condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento", alle "tipologie di dati oggetto del trattamento" agli interessati ed ai "soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati" e, soprattutto, alle "limitazioni della finalità", ai "periodi di conservazione" ed alle operazioni e procedure di trattamento"[61].

Inoltre, va ricordato che l'art. 23 del G.D.P.R. ammette la possibilità, in via generale, per il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento di prevedere misure legislative che limitino la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, purché "tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare", tra gli altri, alla lett. e), "importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale".

Sembra, peraltro, che detti margini di intervento regolatorio siano stati già in parte sfruttati dal Legislatore italiano andando a modificare, nella temperie della crisi pandemica, il testo dell'art. 2 ter del D.Lgs. n 196 del 2003 (il cd. Codice in materia di protezione dei dati personali) in tema di "Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso

[61] Il contenuto della previsione è precisato dal Considerando 45 del G.D.P.R. ove si legge che "È opportuno che il trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri sia basato sul diritto dell'Unione o di uno Stato membro. Il presente regolamento non impone che vi sia un atto legislativo specifico per ogni singolo trattamento. Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo giuridico cui è soggetto il titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire la finalità del trattamento. Inoltre, tale atto legislativo potrebbe precisare le condizioni generali del presente regolamento che presiedono alla liceità del trattamento dei dati personali, prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire se il titolare del trattamento che esegue un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri debba essere una pubblica autorità o altra persona fisica o giuridica di diritto pubblico o, qualora sia nel pubblico interesse, anche per finalità inerenti alla salute, quali la sanità pubblica e la protezione sociale e la gestione dei servizi di assistenza sanitaria, di diritto privato, quale un'associazione professionale".

all'esercizio di pubblici poteri", introducendovi, a mezzo del D.L. 8 ottobre 2021, n. 139 (il cd. "decreto capienze")[62], un nuovo comma 1 bis. Quest'ultima previsione stabilisce, oggi, che "il trattamento dei dati personali da parte di un'amministrazione pubblica […] è sempre consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti" con la precisazione che la "finalità del trattamento, se non espressamente prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento è indicata dall'amministrazione […] in coerenza al compito svolto o al potere esercitato".

È chiara, in essa, l'intenzione del Legislatore di superare una logica di rigida tipizzazione *ex ante* delle possibili basi giuridiche del trattamento dei dati da parte della Pubblica Amministrazione, così abbattendo le barriere all'impiego dei *big data* nell'adozione delle scelte amministrative.

Si tratta di un intervento legislativo non pensato espressamente per la tecnologia dei registri distribuiti ma che invita a riflettere al tema, più in generale, delle modalità con cui fissare, sul versante interno, la disciplina di funzionamento delle *blockchain* amministrative (e non solo con riguardo al profilo della *G.D.P.R. compliance* qui oggetto di approfondimento). Essa potrebbe essere prevista in via unitaria con legge formale ordinaria oppure affidata, anche per fronteggiare i rischi di obsolescenza, a fonti di rango secondario di tipo regolamentare. Meno opportuno appare, per contro, rimettere la disciplina di funzionamento del registro distribuito alla singola *lex specialis* della procedura (come il bando nelle procedure selettive) in quanto, attraverso una parcellizzazione del relativo regime giuridico, ci si allontanerebbe dalla creazione di uno standard disciplinatorio uniforme, invero cruciale anche nell'ottica di conseguire l'obiettivo della interoperabilità tra le singole piattaforme. Non possono, peraltro, sfuggire tutte le evidenti implicazioni anche in punto di tutela giurisdizionale dell'una e dell'altra scelta regolatoria.

In alternativa all'intervento del legislatore nazionale si potrebbe pure ipotizzare, in attesa di una disciplina organica della tecnologia, una modifica puntuale del G.D.P.R. che apra la sua disciplina alla *blockchain*, in maniera non dissimile a quanto sta accadendo, con riferimento all'altro delicato profilo di *compliance* legale delle modalità di identificazione elettronica, con il regolamento eIDAS[63].

È questa, forse, la soluzione preferibile, anche in ragione della sempre maggiore importanza che la tecnologia dei registri distribuiti è destinata a rivestire. Infatti, l'eliminazione a mezzo di un intervento normativo di ogni residuo dubbio applicativo in tema di G.D.P.R. potrebbe, da un lato, rappresentare una spinta verso la concreta applicazione dello strumento (eliminando qualsiasi alibi per la dirigenza, tradizionalmente scettica verso forme di innovazione non espressamente regolate dalla legge) e, dall'altro,

62 Pubblicato in G.U. dell'8 ottobre 2021, n.241.

63 Il riferimento è alla proposta di modifica del Regolamento eIDAS presentata dalla Commissione europea nel giugno 2021 che prevede, ai nuovi articoli 45 *nonies* e *decies*, una disciplina specifica in tema di effetti giuridici dei registri elettronici e di requisiti per i registri elettronici qualificati.

contribuire alla diffusione di un linguaggio amministrativo omogeno a livello unionale che agevoli il sempre più frequente ricorso al modello dell'amministrazione congiunta.

Si aggiungerebbe, così, un ulteriore tassello della nascente e frastagliata disciplina eurounitaria in materia di amministrazione digitale[64], alla cui definizione è chiamata, sul piano teorico e di sistematizzazione, anche la dottrina.

64 Insieme al già citato Regolamento eIDAS. Si pensi anche al tema della cd. "riserva di umanità" rispetto alle funzioni amministrative automatizzate posta proprio dall'art. 22 del G.D.P.R., indicato dal Consiglio di Stato italiano a fondamento della nota sentenza Cons. Stato, Sez. VI, 8 aprile 2019, n. 2270 (con commento di A. G. OROFINO, G. GALLONE, *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, in *Giur. It.*, 7, 2020).