Alessandro Billi(*)

IL TRATTAMENTO DI DATI PERSONALI TRA GDPR E TECNOLOGIE A REGISTRO DISTRIBUITO

Abstract: The article examines the delicate intersection of data protection regulation and blockchain technology. It begins with an introduction to the necessity of data protection, referencing the European Data Protection Regulation No. 679/2016 (GDPR). It then explores the impact of blockchain technology on data privacy, addressing challenges faced by data controllers and processors in navigating the realm of pseudonymization. The exploration extends to the complexities surrounding international data transfers and jurisdictional considerations in a blockchain-driven landscape. The article also discusses the rights to rectification, erasure, and access under GDPR, concluding with the potential for a complex yet fruitful coexistence between data protection laws and blockchain technology.

1. — *Premessa.*

Nel corso degli ultimi due decenni l'avvento, l'espansione e l'evoluzione di internet hanno elevato le tematiche attorno alla privacy, del diritto alla riservatezza e del trattamento dei dati personali, rendendole sempre più complesse, intricate e delicate. Ciò ha condotto l'argomento al centro della discussione, provocando numerose elaborazioni e contributi sul versante giuridico oltre che tecnico, nonché dibattiti dottrinali, anche sulla

(*) Università degli Studi di Perugia.

spinta di una nuova sensibilità diffusa da parte degli utenti, con particolare enfasi sul tema dell'archiviazione e sfruttamento dei dati personali.

Il sorgere, con l'arrivo del c.d. *Web 2.0*[1], di grandi piattaforme informatiche centralizzate, rappresentate dai motori di ricerca più avanzati come Google e Bing, dai social network come Facebook ed Instagram, i servizi di e-commerce come Amazon ed Ebay oppure di sharing, o meglio *aggregating economy*[2] come Uber e AirBnb, ha comportato un interscambio mondiale di dati imponente[3], consentendo ad alcuni fornitori di servizi di prenderne possesso in grande quantità, spesso anche ben oltre le finalità del trattamento di volta in volta necessario.

Ciò ha originato un utilizzo di questi ultimi dal punto di vista commerciale, con tutta l'evoluzione successiva, dal florido e controverso mercato dei c.d. *big data*, sino alla creazione di società specializzate nell'elaborazione dati finalizzata a svolgere attività di *profilazione*[4].

Il dato ha così assunto un valore economico rilevante in svariati contesti, passando dalla realizzazione di pubblicità mirate, sino all'analisi politica[5].

---

[1] Convenzionalmente, lo sviluppo del World Wide Web viene riassunto in fasi, delimitate da discontinuità solitamente costituenti un'evoluzione tecnologica rilevante. La fase del web 1.0 si estende dalle origini del primo sito internet, il 6 agosto 1991, ancora consultabile all'indirizzo *info.cern.ch/hypertext/WWW/TheProject.html*, sino a tutta la sua diffusione. La seconda fase ha inizio invece nel terzo millennio, con il cambio di paradigma: l'utente diviene il protagonista. Fanno la loro comparsa i grandi servizi come e-commerce e social network.

[2] Cfr. *Can We Stop Pretending the Sharing Economy Is All About Sharing?*, reperibile in *Money.com*.

[3] Secondo alcune stime, nel solo 2020 ogni utente ha prodotto mediamente 1,7 megabytes di nuovi dati al secondo, per un totale di circa 44 zettabytes, cioè 440 miliardi di gigabyte: *medium.com/babb/data-blockchain-and-privacy-by-design-454a72319433*.

[4] La profilazione è stata definita dal Reg. UE 2016/679, all'art. 4, par. 1, n. 4, come «qualsiasi forma di trattamento automatizzato di dati personali, utilizzando tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione, gli spostamenti di detta persona fisica».

[5] P. De Filippi, *The interplay between decentralization and privacy: the case of blockchain technologies*, Berkman Center for Internet & Society at Harvard, Parigi, 2016 (*ssrn.com/abstract=2852689*), p. 2 ss.

Molto spesso, il prezzo della gratuità di servizi digitali divenuti ormai quasi imprescindibili nella vita quotidiana, è proprio contenuto nei *Termini e Condizioni* che è obbligatorio sottoscrivere per poterne usufruire, sempre più spesso con la conseguente cessione dei dati personali anche a società terze[6]. Le stime di questo mercato sostengono che per l'anno 2020 tale mercato si è attestato attorno agli 84 miliardi di euro[7].

Internet nel tempo ha dunque assunto la forma di un sistema accentrato, che vede potenti attori ricoprire una posizione pressoché dominante sull'intero settore[8].

2. — *La necessità di protezione dei dati: il regolamento europeo n. 2016/679.*

A seguito del diffondersi dell'attuale paradigma centralizzato, dominante sull'intero mercato e sistema dell'economia digitale, è iniziato il processo, sia sul piano tecnologico che sul versante legale, di elaborazione di strumenti volti a favorire il controllo dei soggetti rispetto ai propri dati personali. Su questa linea uno dei contributi più rilevanti, ma allo stesso tempo controversi, è rappresentato dal nuovo Regolamento europeo sulla protezione dei dati

---

[6] In quest'ottica è divenuta celebre l'espressione «se è gratis, allora il prodotto sei tu», a sottolineare come il dato sia divenuto una vera e propria *commodity,* merce dell'era digitale. Per approfondire il tema sulla Big Data Economy dei grandi colossi digitali, la trasmissione Report ha dedicato un'intera inchiesta giornalistica sui possibili abusi da parte di questi grandi *player* internazionali: *www.report.rai.it/dl/docs/1302771081952prodotto2_pdf.pdf.*

[7] Secondo l'Osservatorio Big Data Analytics & Business Intelligence del Politecnico di Milano, nel 2019, il mercato dei Big Data Analytics in Italia è cresciuto del 23% rispetto all'anno precedente ed è più che raddoppiato rispetto al 2015, raggiungendo la cifra di 1,7 miliardi di euro.

[8] A tal proposito, è stato ripetutamente e da più parti richiesto l'intervento delle autorità antitrust, nello specifico degli USA, al fine di tutelare i consumatori rispetto una *gross negligence of users' privacy*. Tra questi Scott Galloway, professore di marketing alla New York Stern School of Business, ha descritto nel suo saggio i comportamenti di quattro grandi giganti del settore web-tech: Facebook, Google, Amazon, Apple. Cfr. S. Galloway, *The four. I padroni*, Hoepli, Milano, 2018.

personali (reg. UE n. 679/2016) noto con l'acronimo GDPR[9].

Attraverso questo strumento si è voluto porre un freno alla frammentazione normativa in materia, prodotta dalla diversa attuazione nei vari Stati membri della precedente direttiva 95/46/CE[10]. Il regolamento[11] si muove lungo due direttrici fondamentali: dal lato *service provider*, cioè il fornitore dei servizi, viene concepito un sistema con intermediari centralizzati, i c.d. *titolari e responsabili del trattamento*; dal lato utente viene invece fornita agli interessati una serie di strumenti atta ad innalzare il livello di consapevolezza circa l'utilizzo dei propri dati[12]. Riguardo il primo punto, il legislatore europeo ha adottato un nuovo concetto di rischio, seguendo la logica del *one size fits for all*, cioè elaborando un singolo modello valido per tutte le situazioni, a discapito di quella che è la frammentarietà e le peculiarità all'interno del settore, ove insiste il principio di *accountability,* ossia la responsabilità che incombe sul titolare, oggi ancor più accentuata rispetto al passato. Il rischio non si limita più alla fase di violazione, ma si estende anche a quella precedente, in cui il dato potrebbe essere violato sulla base di determinati rischi che spetta al titolare valutare, introducendo una serie di accorgimenti precauzionali.

La prevenzione si ripartisce poi nei due concetti previsti dall'art. 25: quello di *data protection by design*, cioè predisposta sin dalla progettazione del servizio, e quello di *data protection by default*, che si sviluppa mediante impostazioni predefinite finalizzate alla sicurezza dei dati.

Quanto al lato del fruitore, il GDPR rappresenta un significativo tentativo di riequilibrare i ruoli, con una serie di garanzie e strumenti quali l'obbligo di essere sottoposti ad informativa «trasparente, intellegibile e facilmente accessibile», la possibilità di tempestiva segnalazione di invio o vendita di

---

[9] GDPR: per una panoramica completa: G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

[10] Reperibile per intero in *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/432175*.

[11] Entrato in vigore il 25 maggio 2018, consultabile integralmente in *eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA&toc=OJ:L:2016:119:TOC*.

[12] A.M. Gambino, C. Bomprezzi, *Blockchain e protezione dei dati personali*, in *Dir. inf. e inform.*, 2019, p. 619.

dati a terzi, la possibilità di restringere o ritirare il proprio consenso al trattamento, la rettifica di informazioni incomplete od errate, fino ad arrivare al riconoscimento del discusso *diritto all'oblio*[13]. Anche il diritto di accesso viene ampliato, sia dal lato del contenuto, sia mediante il diritto di richiedere e di ottenere una copia dei propri dati personali sottoposti a trattamento.

Tutte queste innovazioni si innestano in uno scenario legislativo la cui ratio è la trasformazione del cittadino da inconsapevole spettatore a soggetto cosciente ed al centro dei processi di gestione dei propri dati[14].

3. — *L'impatto dell'architettura blockchain.*

La realtà appena descritta viene a scontrarsi irrimediabilmente con l'avvento e la diffusione della tecnologia blockchain. Sebbene originata come meccanismo alla base del sistema di pagamento Bitcoin, non solo denaro, ma potenzialmente qualsiasi dato può essere registrato e trasmesso sulla catena, inclusi quelli personali.

Il Parlamento Europeo ha subito dimostrato interesse a questa archi-

---

[13] Con questa ultima espressione si intende una particolare forma di garanzia che prevede la non diffusione, senza la presenza di particolari motivi, di informazioni che possono costituire un precedente pregiudizievole dell'onore di una persona, per tali intendendosi principalmente i precedenti giudiziari di una persona. L'art. 17 disciplina chiaramente i casi in cui deve essere effettuata la cancellazione su richiesta dell'interessato che il titolare del trattamento deve obbligatoriamente concedere "senza ingiustificato ritardo". La richiesta dell'interessato non deve essere in contrasto con altri principi meritevoli di tutela, come quello all'informazione e libertà di espressione. L'Autorità italiana Garante per i Dati Personali si era espressa verso una responsabilità dei motori di ricerca come Google, ove è possibile reperire i collegamenti a queste informazioni. Con recente e discussa pronuncia del 24 settembre 2019 la Corte di giustizia dell'Unione Europea ha però stabilito che questi, qualora dovessero accogliere una richiesta di deindicizzazione da parte di un utente residente nell'Unione Europea, non sono obbligati ad applicarla anche alle ricerche condotte su scala globale.

[14] G. Rugani, *Il diritto all'oblio dell'articolo 17 Regolamento (UE) 2016/679: una grande novità? Una denominazione opportuna?*, in A. Mantelero, D. Poletti (a cura di), *Regolare la tecnologia. Il Reg. Ue 2016-679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa, 2018, p. 455.

tettura informatica, pubblicando già nel febbraio 2017 un report, nel quale vengono formulate ipotesi circa gli ambiti applicativi in cui la blockchain può rappresentare un'importante evoluzione tecnologica per il cittadino, individuando i settori dove può avere maggiore impatto[15]. È stato inoltre sottolineato come le tecnologie più evolute consentono di gestire perfino interi software, gli *smart contract*, che possono essere in un certo senso assimilati ad accordi contrattuali. Nel momento in cui i dati personali vengono trattati attraverso queste *Digital Applications*, basate su blockchain, è chiaro come venga in essere un rapporto regolato dal GDPR, con non poche problematiche connesse da un lato rispetto alle peculiarità della tecnologia, dall'altro rispetto l'impianto legislativo sotteso dal regolamento.

L'art. 25 GDPR, nella parte relativa alla c.d. *data protection by design*, richiede al titolare del trattamento di mettere in atto «misure tecniche e organizzative adeguate, quali la pseudonimizzazione[16], volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione[17], e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente Regolamento e tutelare i diritti degli interessati»[18].

---

[15] Il report, intitolato *How blockchain technology could change our lives'* è reperibile integralmente in *www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf*.

[16] Con pseudonimizzazione si intende «il trattamento dei dati personali in modo tale che essi 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» (art. 4, par. 1, n. 5 GDPR).

[17] La minimizzazione dei dati prevede che i dati personali siano «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (art. 5, par. 1, lett. *c)* GDPR).

[18] La disposizione viene integrata nel considerando n. 78, per cui si prevede che le misure potrebbero consistere nel: ridurre al minimo il trattamento dei dati personali; pseudonimizzare i dati personali il più presto possibile; offrire trasparenza per quanto riguarda le funzioni ed il trattamento di dati personali; consentire all'interessato di controllare il trattamento dei dati; consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. Sul punto si sono pronunciati favorevolmente alcuni studiosi, tra cui: M. Berberich, M. Steiner, *Blockchain technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?*, in *European Data Protection Law Review*, 2016, p. 425.

Partendo da queste premesse, apparrebbe che la blockchain possa soddisfare le linee programmatiche del GDPR, costituendo uno strumento utile ed adatto per garantire la sicurezza e l'integrità dei dati in essa contenuta. Un registro così decentrato si dimostrerebbe inoltre più resistente ad eventuali attacchi informatici o a malfunzionamenti rispetto a una soluzione tradizionale[19].

Per queste ragioni, nella Dichiarazione Istitutiva della Blockchain Partnership europea, siglata da 22 stati membri per cooperare sugli sviluppi futuri in materia, viene affermato che «i servizi blockchain-based aiuteranno a preservare l'integrità dei dati e garantiranno una migliore gestione degli stessi da parte dei cittadini e delle organizzazioni che interagiscono con le pubbliche amministrazioni»[20]. Il Parlamento Europeo si è poi nuovamente pronunciato sull'argomento, con Risoluzione del 3 ottobre 2018[21], dichiarando che la blockchain possa «costituire uno strumento che rafforza l'autonomia dei cittadini dando loro l'opportunità di controllare i propri dati e decidere quali condividere nel registro, nonché la capacità di scegliere chi possa vedere tali dati».

Tuttavia, è sempre nello stesso documento che viene posta in evidenza la presenza di più di un elemento di incompatibilità tra blockchain e GDPR.

Al contrario di un tradizionale servizio informatico, nel quale i dati vengono conservati in un server centrale, questa si basa su di un'infrastruttura *peer-to-peer* in cui le informazioni sono distribuite nella rete degli utenti. In

---

[19] Tuttavia è importante evidenziare come non ci si trovi comunque dinnanzi ad un sistema impossibile da *bypassare*. Sebbene estremamente difficile, è comunque possibile risalire alla stringa alfanumerica della chiave privata. Attraverso la scoperta e la ricostruzione di una chiave privata non si identificherebbe immediatamente una persona fisica, costituendo solamente qualche cosa che quest'ultima conosce e gestisce, anche se l'apprensione della chiave privata comporta la disponibilità di spendere ciò che è connesso a tale chiave. L'indirizzo, dunque, costituisce uno pseudonimo, cioè una rappresentazione intermedia, non direttamente collegabile al soggetto titolare. Cfr. R. Battaglini, M.T. Giordano, *Blockchain e Smart Contract*, Milano, 2019, p. 100.

[20] A.M. Gambino, C. Bomprezzi, *Blockchain e protezione dei dati personali*, cit., p. 623.

[21] Risoluzione dal titolo *Tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione*, reperibile integralmente in *www.europarl.europa.eu/doceo/document/TA-8-2018-0373_IT.pdf?redirect*.

una blockchain come prevista dal modello "originale", cioè pubblica e *permissionless*, la caratteristica intrinseca della trasparenza fa in modo che i dati, oltre che immutabili, siano accessibili ad un vasto numero di soggetti[22]. Da un lato quindi la natura trasparente e distribuita sembra essere uno dei punti di forza di questa tecnologia. D'altro canto però, il suo funzionamento tramite la catena di blocchi, e dunque la replica di dati su tutte le copie del registro, confligge apertamente con il *principio di minimizzazione dei dati*. Il GDPR prevede infatti che i dati e le loro copie siano limitati a quanto necessario rispetto alle finalità per le quali sono trattati. In sostanza, le informazioni raccolte devono essere adeguate e pertinenti rispetto al fine che si intende perseguire, e non possono essere acquisite in misura maggiore a quella necessaria. Ciò non può essere in alcun modo rispettato nel normale funzionamento del registro di una blockchain permissionless, che dunque si trova in palese contrasto con i principi di *data protection by design* ed *accountability*.

Nelle blockchain permissionless la chiave privata per accedere alle informazioni, da coordinare con quella pubblica, è in possesso e di responsabilità esclusiva della persona fisica di riferimento, senza che nessun intermediario o ente centrale possa conoscere la correlazione tra questa ed il suo utilizzatore.

Riguardo le chiavi pubbliche invece, che hanno una funzione simile a quella degli *account*[23] dei servizi tradizionali e che sono costituite da una stringa di numeri e lettere generalmente in ordine casuale[24], alcuni autori

---

[22] M. Berberich, M. Steiner, *Blockchain technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?,* cit., p. 425.

[23] Ciò si ricollega, relativamente al dibattito riguardante un'altra tecnologia, al dibattito circa la natura dell'indirizzo IP dinamico quale dato personale. La questione è stata risolta in senso positivo solo anni dopo, con sentenza *Breyer* della Corte di Giustizia dell'Unione Europea del 16 ottobre 2016.

[24] Per la verità, esistono servizi online che permettono di generare delle chiavi contenenti al loro interno una parte della stringa richiesta dall'autore (ad esempio il proprio nome o altri riferimenti). L'adozione di tale possibilità è sconsigliata dagli esperti del settore, in quanto aumenterebbe ancor più l'esposizione al rischio di essere rintracciati. Aspetto emerso nel corso del webinar *Blockchain* tenuto da Sistemi Formativi Confindustria Umbria presso Umbria Business School in data 17 aprile 2020.

hanno sostenuto che si realizzerebbe una forma di pseudonimizzazione[25]. Ciò, in aggiunta al fatto che i dati contenuti nei blocchi sono criptati, escluderebbe l'applicazione del GDPR, in quanto si è in presenza di informazioni riconducibili a dati anonimi.

Questa tesi, nonostante l'indubbio sforzo interpretativo, non può essere sostenuta per una serie di ragioni. Innanzitutto, non è così infrequente che sia possibile ricollegare l'indirizzo ad una specifica identità. Ciò può avvenire per esempio nel caso in cui questo sia presente in una pagina pubblica, come un sito web o un forum, ai fini dello scambio di criptovalute[26]. In aggiunta, vi è da segnalare che esiste un settore in rapido sviluppo, quello delle cc.dd. *blockchain analysis e digital forensic,* finalizzato allo sviluppo di procedimenti investigativi volti a risalire a identità apparentemente anonime, utili anche in contrasto ad attività illecite come il riciclaggio di denaro[27].

Per quel che riguarda invece il contenuto dei singoli blocchi, che rappresentano "agglomerati" di dati, occorre poi considerare che né la crittografia, né la funzione di *hash,* possono essere reputate totalmente anonime, risul-

---

[25] Tra gli altri, N. Fabiano, *The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard*, 2017, International Conference on Internet of Things for the Global Community (IoTGC), Funchal, 2017, pp. 1-7.

[26] Ciò è la comune prassi in alcune piattaforme di exchange specializzate, come Coinbase, società californiana che opera scambio di Bitcoin, Ethereum, LiteCoin ed altri beni digitali con valute in corso legale in 32 nazioni.

[27] Alcune società come Coinalytics, Coinometrics o Elliptic ne hanno fatto il fulcro del loro business. La blockchain può essere sottoposta a diverse tipologie di indagine, delle quali la più ardua, ma penetrante, è sicuramente quella circa l'identità del proprietario di un indirizzo, che necessita di una serie di analisi incrociate. Una delle principali tecniche di deanonimizzazione è rappresentata dal *clustering,* cioè l'identificazione di vari indirizzi riconducibili presumibilmente ad uno stesso *wallet*, collezione di indirizzi appartenenti ad una stessa entità. Per un quadro completo circa le modalità di approccio si rimanda a: J.D. Nick, *Data-Driven De-Anonymization in Bitcoin*, Distributed Computing Group Computer Engineering and Networks Laboratory ETH, Zurigo, 2015. Vari strumenti sono stati inoltre predisposti al fine di automatizzare parzialmente l'indagine, come il gratuito WalletExplorer, o l'italiano XFlow, acquisito nel 2019 da Coinbase. Come risposta all'evolversi di queste tecniche si è assistito alla nascita di varie criptovalute che rendono quasi impossibile l'attività di deanonimizzazione tra cui Monero e Zcash. Per approfondire l'argomento: R. Battaglini, M.T. Giordano, *Blockchain e Smart Contract*, cit., p. 123.

tando perciò preferibile l'inserimento di questo fenomeno nella categoria dello *pseudoanonimato*[28].

In definitiva, trattandosi dunque di una forma, per quanto raffinata ed avanzata, di *pseudonimizzazione*, i dati in essa contenuti ricadono nell'ambito di applicazione del GDPR. Rimane perciò possibile, per quanto reso particolarmente oneroso, re-identificare il proprietario utilizzando alcune *informazioni aggiuntive*, come richiamate all'art. 4, par. 1, n. 5 GDPR. Per far fronte a queste problematiche e prevenire l'identificazione del titolare della chiave pubblica, sono state elaborate varie strategie, dalle più semplici a soluzioni più complesse, tra le quali l'utilizzo di indirizzi usa e getta, il sistema delle c.d. *ring signatures,* fino alla c.d. *zero knowledge proof*[29]. Bisogna ancora una volta tenere in considerazione come queste tecniche, così come l'intera tecnologia, siano in una fase di continui sviluppi ed evoluzioni, per cui è solamente possibile fotografare la situazione in quel preciso momento.

Discorso parzialmente diverso può essere condotto nel caso di adozione di una blockchain di natura differente, quale il caso di un modello *permissioned*, contraddistinto dalla selezione di chi ha la facoltà di accedervi e chi può visionare le informazioni in essa contenute, sebbene non verrebbe scongiurata neanche in questo caso la moltiplicazione dei dati personali all'interno delle singole copie dei registri posseduti da ogni partecipante alla rete[30].

---

[28] Così come definito dal Gruppo di lavoro *Articolo 29*, organismo consultivo indipendente europeo delle autorità di vigilanza e protezione dei dati, nel suo parere del 10 aprile 2014, consultabile integralmente in *ronchilegal.eu/wp-content/uploads/2017/12/Anonimizzazione-secondo-il-WP29-del-2014_it-1.pdf*.

[29] La prima tecnica prevede l'utilizzo di una chiave diversa per ogni operazione da compiere. Con le *ring signatures* invece ogni firma digitale viene fatta ricondurre non ad un singolo, ma ad un gruppo di utenti. La *zero knowledge proof* si tratta di un particolare tipo di crittografia che non richiede la rivelazione di informazioni sensibili per la validità della transazione. Il sistema viene utilizzato dalla tecnologia Zcash. Cfr. M. Finck, *Blockchains and Data Protection in the European Union*, Monaco di Baviera, 2017, p. 15.

[30] Si è espressa in tal senso la Commission Nationale Informatique & Libertés francese, attraverso il documento *La Blockchain: quelles solutions pour un usage responsable en présence de données personelles?*, pubblicato in data 24 settembre 2018.

Taluni autori[31] ritengono che, in base alla lettera del considerando 26 GDPR[32], sia possibile ipotizzare di ritenere soddisfatti i principi di *accountability* e minimizzazione, rendendo così possibile una valutazione positiva della tecnologia blockchain. A tal fine sarebbe necessaria l'effettuazione di un'analisi finalizzata a valutare parametri oggettivi, come i costi ed il tempo necessari da dedicare a eventuali operazioni di re-identificazione, considerando i mezzi disponibili allo stato dell'arte attuale. Quello che risulta però al momento, elemento che può definirsi condiviso da gran parte delle declinazioni di questa architettura, è la difficoltà ad assicurare un elevato tasso di improbabilità nella re-identificazione partendo da un indirizzo, tenuto conto anche della giovinezza di tale tecnologia. Per questa serie di ragioni, rimane unanimemente sconsigliabile, almeno allo stato attuale, la conservazione dati personali e sensibili su blockchain, in special modo di tipo *permissionless*.

4. — *Titolare e responsabile del trattamento alla prova dello pseudoanonimato.*

Continuando la disamina degli elementi di frizione tra il GDPR e le peculiarità della blockchain, veniamo ora ad uno dei punti più spinosi del dibattito: l'individuazione del titolare e del responsabile del trattamento. Analizzando il Regolamento emerge con vigore quanto sia centrale per il legislatore europeo il ruolo del *service provider,* il quale è soggetto ad una serie di oneri e responsabilità. Il Regolamento definisce quale titolare «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»[33]. Con finalità si intende la motivazione dell'utilizzo dei dati, mentre con mezzi vengono indicate le modalità tecniche ma anche organiz-

---

[31] A.M. Gambino, C. Bomprezzi, *Blockchain e protezione dei dati personali*, cit., p. 636.

[32] Nella parte in cui si dispone che «*Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici*».

[33] Art. 4, 1° comma, n. 7, GDPR.

zative del trattamento, come l'individuazione di chi ha effettivo accesso ai dati. È possibile, ed anzi, frequente, che più soggetti siano titolari del trattamento, in una situazione di *contitolarità*.

Sull'altro versante, la figura del *responsabile* è invece rappresentata da colui che «*tratta i dati personali per conto del titolare del trattamento*», secondo le finalità e le indicazioni impartite da questo[34].

Considerate le succitate caratteristiche di una blockchain permissionless, la sua natura distribuita, la capacità di disintermediazione e di pseudoanonimato dei partecipanti[35], è improbabile non ravvedere un'obiettiva difficoltà nel rintracciare la precisa identità del titolare del trattamento.

A tale riguardo si sono sviluppate in dottrina due ricostruzioni opposte. Secondo alcuni autori[36], non esisterebbe un'entità individuabile che abbia la potestà di predeterminare gli usi e governare il sistema, in quanto ogni nodo è uguale all'altro. Per questa ragione, verrebbero a mancare degli elementi essenziali affinché possa ritenersi soddisfatto il requisito dell'*accountability*. Questa visione si presta però a delle critiche ben supportate[37].

A opinione di altri autori[38], ogni nodo dovrebbe invece essere considerato titolare dei dati per sé stesso e *data processor*, responsabile per gli altri nodi, in quanto, detenendo copia dei dati e contribuendo al mantenimento di questi nel registro, configurante un elemento strumentale e di ausilio al trattamento[39].

Riconoscendo la titolarità del trattamento al singolo nodo, tuttavia, non si prende in considerazione che questo in realtà non è dotato di un potere

---

[34] C. Del Federico, A.R. Popoli, *Disposizioni generali*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 89 ss.

[35] Il titolare del trattamento potrebbe affidare ad un altro soggetto la costruzione dell'infrastruttura. Costui potrebbe assumere poi il ruolo di responsabile del trattamento.

[36] Tra cui J. Moser, *The Application & Impact of the European General Data Protection Regulation on Blockchains*, in *R3 Reports*, 2017, p. 9.

[37] A.M. Gambino, C. Bomprezzi, *Blockchain e protezione dei dati personali*, cit., p. 641.

[38] Tra questi anche M.T. Giordano, *La blockchain ed il trattamento dei dati personali*, in R. Battaglini, M.T. Giordano, *Blockchain e Smart Contract*, cit., p. 105.

[39] In questo senso, M. Finck, *Blockchains and Data Protection in the European Union*, cit.

irrevocabile di intervento sul trattamento dei dati, come ad esempio, citando uno dei possibili risvolti sul piano concreto, nell'ottemperare la richiesta di rettifica o cancellazione delle informazioni. Per realizzare queste operazioni sarebbe necessario rispettare il meccanismo del consenso previsto dal modello di blockchain, risultate nel caso più frequente nel raggiungimento della maggioranza dei nodi, che viene stabilito solamente a monte, in sede di programmazione, dagli sviluppatori del software stesso. Anche questa tesi dunque, nonostante i lodevoli propositi, non fa altro che mettere in luce quanto sia difficile modellare il Regolamento europeo, almeno allo stato attuale, sul paradigma di una blockchain "originale".

Questa rende ardua la definizione puntuale dei ruoli dei propri partecipanti, in assenza di un nodo che rappresenti il vero *dominus* della rete, in ragione delle caratteristiche base dell'architettura, il libero accesso e la natura *open source*. In tale situazione il GDPR, pur astrattamente applicabile, appare difficilmente adattabile a questa nuova architettura[(40)].

Discorso inverso va invece fatto qualora l'architettura prescelta sia una blockchain totalmente privata, in cui il titolare coincide con il gestore dell'infrastruttura, cui spetterebbe la determinazione delle finalità e dei mezzi del trattamento, così come anche nell'ipotesi di blockchain pubblica *permissioned*, dove è possibile ravvisare la presenza di un soggetto in grado di selezionare gli accessi, il livello di trasparenza e di monitorare i nodi e le loro attività[(41)]. Costui può essere dunque assimilato al ruolo di titolare (o contitolari se si

---

(40) Con l'intento di risolvere alla radice questo problema, la Commission Nationale Informatique & Libertés, autorità garante per la protezione dei dati personali francese, nel documento esplicativo emesso a novembre 2018 e intitolato *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data* ha ritenuto di poter applicare, nella maggioranza dei casi, l'esenzione dalle norme del Regolamento prevista all'art. 2, 2°comma, lett. *c)* per i trattamenti c.d. *domestici*: tale esenzione permetterebbe di non considerare i trattamenti svolti dai privati come ricadenti sotto le rigide disposizioni di cui al GDPR e, pertanto, di non dover considerare i nodi (ove gestiti da utenti non professionali) veri e propri responsabili del trattamento. Stesso ragionamento si applicherebbe ai miner, che vengono in questo quadro considerati (non senza qualche dubbio interpretativo) come meri validatori di transazioni altrui e, in quanto tali non titolari di alcun ruolo di responsabilità.

(41) A.M. Gambino, C. Bomprezzi, *Blockchain e protezione dei dati personali*, cit., p. 638.

trattasse di più soggetti)[42]. In questi due modelli il responsabile sarebbe poi individuato attraverso la nomina da parte del titolare.

5. — *Trasferimento di dati all'estero ed individuazione della giurisdizione.*

Un altro aspetto di rilievo circa l'applicazione del GDPR ad un'infrastruttura blockchain riguarda le questioni di giurisdizione ed il trasferimento di dati all'estero. Il Regolamento struttura un vasto ambito di applicazione territoriale, che impone l'individuazione *ab origine* e in modo predeterminato della legge applicabile al caso concreto. A norma dell'art. 3, questo procedimento si applica anche qualora il trattamento venisse posto in essere fuori dall'Unione Europea, ma sia collegato ad attività svolte dal titolare o responsabile del trattamento che ha sede in uno degli Stati membri[43]. Lo stesso avviene nel caso in cui l'interessato si trovi all'interno dei confini europei, ma il titolare o il responsabile non hanno uno stabilimento nell'Unione[44]. Se questo procedimento appare perfettamente eseguibile in sistemi accentrati di rete e di servizi, è stato evidenziato precedentemente già come solo l'individuazione del titolare e del responsabile del trattamento di una blockchain permissionless sia molto ardua.

La natura globale, incoercibile e pseudoanonima rende altresì molto complesso verificare il luogo del trattamento e dello stabilimento.

L'identità dell'interessato viene inoltre occultata dietro una stringa alfanumerica, per cui non è semplice stabilire se egli si trovi o meno nel territorio dell'Unione, anche se in questo caso sarebbe sufficiente stabilire un

---

[42] Cfr. C. Bomprezzi, *Blockchain e assicurazione: opportunità e nuove sfide*, in *Dir., merc., tecnologia*, 2017, p. 29.

[43] Ciò si applica «quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione».

[44] Lo stesso avviene anche quando il trattamento viene posto in essere da un titolare non stabilito nell'Unione, in un luogo che secondo il diritto internazionale pubblico è soggetto al diritto di uno Stato membro.

criterio di collegamento, ad esempio basandosi su elementi come la presenza di un nome di dominio europeo[45].

Anche in questo caso, la scelta di una blockchain privata o pubblica *permissioned* consentirebbe invece la possibilità di individuare titolare e responsabile del trattamento, nonché l'identificazione del soggetto interessato, così risultando applicabile il GDPR senza ulteriori operazioni.

Quanto alla questione riguardante il trasferimento dei dati personali, il discorso fatto finora va integrato con un ulteriore approfondimento sul funzionamento stesso dell'infrastruttura blockchain. I dati inseriti nei blocchi vengono uniti alla catena tramite il *nodo validatore*, prima di essere replicati nelle varie copie del registro. Il problema giuridico in questo caso, oltre al discorso già affrontato precedentemente circa la localizzazione del nodo, è se possa ritenersi realizzato o meno un *trasferimento*[46] di dati personali ai sensi degli artt. 44 ss. GDPR[47].

Estendendo quanto enunciato nella criticata sentenza *Bodil Lindqvist*[48] della Corte di Giustizia dell'Unione Europea alla blockchain, parte della dottrina esclude che ciò possa dirsi perfezionato, considerando che «i dati non sono trasferiti direttamente, ma all'esito di un processo di validazione e successiva replica nei nodi della blockchain».

---

[45] A.M. Gambino, C. Bomprezzi, *Blockchain e protezione dei dati personali*, cit., p. 643.

[46] Il GDPR non fornisce una definizione di "trasferimento", la quale è stata elaborata per differenza rispetto al concetto di "comunicazione". Con quest'ultima vengono identificati gli spostamenti di dati tra titolari, all'interno dell'Unione. Il trasferimento si configurerebbe dunque con i movimenti di dati tra soggetti, titolari o responsabili, con la presenza di almeno uno di essi fuori dai confini europei. A tal proposito, M.C. Meneghetti, *Trasferimenti di dati personali*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 436.

[47] W. Maxwell, J. Salmon, *A guide to blockchain and data protection*, Hogan Lovells, Londra-Washington, 2017, p. 16.

[48] Decisione riguardante il trasferimento di dati personali mediante pagina internet caricata presso un web hosting provider stabilito nello Stato stesso o in un altro Stato membro. In quel caso la Corte negò che l'inserimento di dati personali in un sito web possa essere qualificato come trasferimento. Le maggiori critiche hanno riguardato il mancato chiarimento circa alcuni importanti aspetti, quali se i dati venissero materialmente scaricati su un computer di un Paese Terzo, oppure se l'hosting provider fosse ivi stabilito.

In quella vicenda, la Corte enunciò il principio che «i dati personali che giungono al computer di una persona che si trova in un Paese Terzo […] non sono stati trasferiti direttamente tra queste due persone, ma attraverso l'infrastruttura informatica del fornitore di servizi di ospitalità». A causa di questa "mediazione" da parte del *web hosting provider* quindi, non si configurerebbe un trasferimento.

Allo stesso modo, il fatto che i dati di una blockchain non vengono trasferiti direttamente, ma all'esito del succitato processo di validazione e successiva replica, escluderebbe anche in questo caso il trasferimento[49]. Appare tuttavia uscire rafforzata anche in questa situazione la necessità di un cambio di paradigma normativo, presa coscienza di come ci si trovi di fronte a luoghi virtuali insuscettibili per natura ai confini delle giurisdizioni, nei quali gli attori si muovono in un ambiente dominato dalle regole della *lex cryptographica*.

6. — *Diritto di rettifica e cancellazione.*

Passando in rassegna altri aspetti chiave del nuovo sistema normativo predisposto dal legislatore eurounitario, è stato sottolineato in precedenza come il GDPR conferisca al singolo *interessato* una serie di strumenti atti ad acquisire coscienza e a poter intervenire sul trattamento dei propri dati. Tra questi, il diritto di *rettifica*[50] e quello di *cancellazione*[51] ai sensi degli artt. 16-17 GDPR, vengono inevitabilmente ad impattare con l'immutabilità della blockchain e la conservazione perpetua dei dati in essa.

A tale riguardo sono state prospettate diverse soluzioni, sia dal lato informatico che sul versante legale. Sul primo punto, è stato sperimentato l'utilizzo del c.d. *chameleon hash*, che consentirebbe di mantenere inaltera-

[49] Cfr. A.M. Gambino, C. Bomprezzi, *Blockchain e protezione dei dati personali*, cit., p. 634.

[50] *Ex* art. 16 GDPR, «l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo».

[51] Il diritto alla cancellazione sussiste nel momento in cui «i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati».

to l'hash originale del blocco, pur permettendo di effettuare cambiamenti. Se da un lato ciò renderebbe inoppugnabilmente possibile l'esercizio di tali diritti, non possono essere sottovalutati i risvolti tecnici in negativo in tema di sicurezza dell'intero sistema[52]. Un'altra soluzione verte invece sul significato da attribuire al termine "cancellazione", che secondo alcuni non indicherebbe necessariamente la distruzione fisica del dato, potendo essere realizzata anche tramite l'inaccessibilità dello stesso, realizzabile mediante alcune tecniche, come la conservazione dei dati *off-chain*[53], cioè fuori dalla catena, iscrivendovi solo un collegamento con questi al loro interno, un hash dei dati. La blockchain verrebbe dunque utilizzata per archiviare la prova che alcuni dati esistono piuttosto che memorizzare gli stessi. Ciò consentirebbe la rimozione dei dati personali senza rompere la catena[54].

7. — *Diritto di accesso.*

Altro importante nuovo strumento proposto dal Regolamento è costituito dal diritto di *accesso*, normato dall'articolo 15, che conferisce al portatore di interessi la possibilità di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso a tali dati. Anche in questo caso ci si ricollega al problema dell'individuazione del titolare e del responsabile del trattamento.

In aggiunta, anche se fosse superata questa problematica trattata in precedenza, sarebbe poi allo stesso modo arduo per costui venire a conoscenza con certezza e precisione circa i dati personali sottoposti a trattamento, in quanto coperti dalla crittografia asimmetrica propria della tecnologia.

---

[52] A. Ricci, *I diritti dell'interessato*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., pp. 198-199.

[53] Come proposto da M. Finck, *Blockchains and Data Protection in the European Union*, cit., p. 23 ss.

[54] Cfr. A. Valeriani, *Blockchain vs GDPR: due opposti inconciliabili?*, in *Iusinitinere.it*, 24 ottobre 2018.

Proprio su questo punto però la blockchain potrebbe risultare veramente uno strumento, come ricordato anche dalla recente Risoluzione del Parlamento Europeo, in grado di garantire il diritto di accesso dell'interessato, allo stesso tempo dotato di maggior grado di protezione dei propri dati.

Le caratteristiche di tracciabilità e trasparenza possono conferire infatti al soggetto coinvolto la facoltà di ripercorrere tutti i trattamenti ai quali è stato sottoposto, limitare l'uso dei propri dati a specifiche operazioni, ed all'occorrenza, revocarlo[55]. Sul tema si discute della possibilità di predisporre l'erogazione di importanti servizi pubblici sotto questa forma, come nel caso del fascicolo sanitario elettronico decentralizzato[56].

Anche in termini di integrità del dato, il livello di garanzia di una sua conservazione su blockchain è elevato, in virtù delle caratteristiche base della tecnologia. Si tratterebbe dunque di una vera e propria "responsabilizzazione" del soggetto privato, che diverrebbe sempre più proprietario dei propri dati.

Va inoltre ancora una volta sottolineato che, anche in questa area di studio, l'adozione di una blockchain *permissioned*, semplificherebbe e non poco le problematiche legate all'immutabilità unilaterale della catena, che verrebbero poi totalmente annullate nel caso di una blockchain del tutto privata, o ibrida, magari gestita da una Pubblica Amministrazione, nonostante la perdita di alcune proprietà uniche di una rete pubblica e *permissionless*.

8. — *Una complessa, ma potenzialmente fruttuosa convivenza.*

Arrivati alla conclusione di questa analisi, va ancora una volta evidenziato quanto risulti complesso e gravoso il compito del diritto quando messo di fronte ad innovazioni tecnologiche così repentine, chiamato a essere in gra-

---

[55] L.D. Ibáñez, K. O'Hara, E. Simperl, *On Blockchains and the General Data Protection Regulation*, Report, Southampton, Luglio 2018, p. 11.

[56] S. Tallarico, B. Nicolai, Applicazioni blockchain per la condivisione e archiviazione dei dati: sfide e opportunità per il Servizio Sanitario Nazionale, contributo in *Convegno Nazionale Associazione Italiana Ingegneri Clinici: Verso un nuovo SSN. Professionisti, Innovazione e PNRR, Health Technology Challenge AIIC 2021, Milano, 2021.*

do di "intercettarle" e a delineare in brevissimo tempo un sistema contemporaneamente efficace alle finalità di tutela, ma allo stesso tempo abbastanza elastico da adattarsi alle inevitabili e continue evoluzioni.

Questa premessa ci è utile se si prende in considerazione che i lavori preparatori del Regolamento Europeo sulla Protezione dei dati personali hanno avuto inizio nel 2012, anno in cui la tecnologia blockchain muoveva i suoi primi passi, non era ancora conosciuta dalla maggior parte degli utenti e, soprattutto, non aveva registrato ancora una diffusione tale da rappresentare un punto focale di cui il legislatore avrebbe necessariamente dovuto tener conto nella stesura delle nuove disposizioni comuni in tema di tutela dei dati personali. All'epoca, l'unica blockchain funzionante era quella di Bitcoin, dove nella sua fase primordiale rarissimamente venivano registrate informazioni quali i dati personali[57].

Il paradigma tecnologico preso in esame dal GDPR è stato dunque quello dominante all'epoca, che rimane tutt'ora il più diffuso, e cioè quel sistema centralizzato, ove l'esistenza di un ente principale rende relativamente semplice l'individuazione di un responsabile del trattamento. Il GDPR, prendendo atto di ciò, ha realizzato un sistema volto a responsabilizzare i grandi *player* del web, nell'ottica di tutelare il cittadino-utente, elaborando un impianto non esente da alcune critiche.

In breve tempo però lo stato delle cose sembra essere sulla via di una nuova fase.

Per questa ragione si renderà inevitabilmente necessaria una revisione dell'intero complesso legislativo, pur se di non facile realizzazione. La presenza sempre più capillare e la fuoriuscita dalla fase prototipale di operatori che forniscono già servizi agli utenti tramite sistemi blockchain non può far altro che stimolare la ricerca e l'elaborazione giuridica, finalizzata a sciogliere gli attuali interrogativi e ad offrire soluzioni che non possono rimanere ancorate al tentativo di adattarvi la normativa attuale e sulla ricerca di figure sovrapponibili in un sistema centralizzato.

---

[57] M.T. Giordano, *La blockchain ed il trattamento dei dati personali*, in R. Battaglini, M.T. Giordano, *Blockchain e Smart Contract*, cit., p. 101.

Preso atto di questa situazione, appare chiaro come sia necessaria una presa di coscienza circa la necessità di un'elaborazione giuridica ad hoc, vera e propria sfida nell'ottica di armonizzare questa tecnologia dirompente con i principi sanciti nelle varie Costituzioni degli Stati membri e nel GDPR.

Nel corso della trattazione è emerso come GDPR e blockchain, a prima vista inconciliabili, possono condividere un obiettivo di fondo comune: creare un ambiente in cui sia mantenuta la sicurezza dei dati e in cui sia restituito ai soggetti il controllo sugli stessi. Come abbiamo poi avuto modo di specificare nel corso della trattazione, le tecnologie DLT e in particolar modo la blockchain, consistono in un insieme di sistemi eterogenei ognuno con le proprie peculiarità e punti deboli, il che rende l'analisi e la predisposizione di normative specifiche ancora più probante ed impegnativa per il giurista, che dovrà anche essere dotato di un corposo bagaglio di conoscenze nel settore di riferimento, in un contesto di sempre maggiore interoperabilità *tecno-legale*.

Alcuni sforzi in questa direzione sono testimoniati dalla grande attenzione che si sta registrando, oltre a livello di grandi investitori privati sotto forma di consorzi e *joint ventures*, anche a livello nazionale e soprattutto internazionale, nonostante il fenomeno sia ancora alle prime battute e non occupi ancora le prime pagine con frequenza. Il particolare rilievo che viene attribuito alle nuove funzionalità in tema di protezione dei dati personali è sostenuto anche dal lavoro in questo ambito portato avanti dall' *Osservatorio e Forum dell'Unione Europea sulla Blockchain*[58], e da una serie di finanziamenti in seno al programma *Horizon 2020* finalizzati alla ricerca.

Anche nei Report annuali del Garante Europeo per la protezione dei dati viene enunciata la scelta di monitorare queste nuove tecnologie, al fine di trarne i maggiori benefici, pur contemperandole con i diritti dei cittadini,

[58] L'Osservatorio ha organizzato a Bruxelles un primo workshop sul tema, dal titolo *Opposites attract: Reconciling GDPR and blockchain*, nel giugno 2018. Successivamente, è stato prodotto anche un report, in cui è stato affermato che il GDPR non può rappresentare la fine della blockchain, e che le tensioni possono essere allentate mediante l'intervento del legislatore, dello European Data Protection Board e della giurisprudenza (T. Lyons, L. Courcelas, K. Timsit, *Blockchain and the GDPR - a thematic report prepared by the European Union Blockchain Observatory and Forum*, Report, Osservatorio Blockchain in seno all'Unione Europea, 2018, cit. p. 28).

non rinunciando ad un'opportuna regolamentazione[59]. La linea tracciata è quella dunque dello sviluppo e dell'adozione di blockchain *privacy-friendly*, che può essere perseguita solo attraverso un dialogo interdisciplinare tra diritto e tecnologia. Rispetto a quest'ultima, sono state evidenziate alcune possibili soluzioni, fino ad arrivare alla scelta piuttosto drastica di optare per il modello privato o *permissioned*, che appare più predisposto alla regolamentazione, sebbene obblighi a qualche rinuncia rispetto all'infrastruttura pubblica e anonima[60].

Sull'altro versante, quello legale, il primo passo da compiere è sicuramente di pervenire alla definizione di un quadro generale e sufficientemente efficace a definire un mondo così nuovo e vasto, formato da pressoché infinite varianti dalle caratteristiche più disparate, aldilà degli interessanti, quanto timidi tentativi intra statali[61].

Vista la globalità, l'ampiezza e la transnazionalità del fenomeno, la soluzione non può che essere trovata attraverso una concertazione a livello europeo ed internazionale. Su questa linea si registra l'attivazione della *Commissione Tecnica 307 sulla blockchain e DLT*[62], con l'obiettivo di elaborare degli standard e progetti anche focalizzati sul tema della protezione dei dati personali, sotto l'egida *dell'ISO, Organizzazione Internazionale per la normazione*, la più importante a livello mondiale per la definizione di norme tecniche, alla quale partecipano 164 Stati. A livello europeo si sono invece mossi il

---

[59] Entrambi i report sono disponibili sul portale ufficiale del Garante Europeo della protezione dei dati, all'indirizzo *edps.europa.eu/annual-reports_en*.

[60] H. Halpin, M. Pietraska, *Introduction to Security and Privacy on the Blockchain*, 2nd Ieee European Symposium on Security and Privacy Workshops, Parigi, 2017, pp. 1-3.

[61] Diversi Stati del mondo hanno iniziato a definire le nuove tecnologie, soprattutto ai fini di normative legate a settori come il fin-tech. Per citare alcuni esempi all'interno dell'Unione Europea, si ricordano, oltre l'Italia con il Decreto Semplificazioni del 2019, Malta, che nel 2018 ha approvato tre leggi a riguardo, e la Francia, attiva già dal 2016 con una serie di ordinanze sulla registrazione e trasferimento di titoli finanziari non quotati mediante blockchain.

[62] Lo stato dei lavori, in continua evoluzione è consultabile all'indirizzo *www.iso.org/committee/6266604.html*.

Comitato Europeo di normazione (CEN)[63] insieme al *Comitato Europeo di normazione elettrotecnica (CENELEC)*[64], attraverso un documento congiunto[65] con l'obiettivo di fornire alle istituzioni eurounitarie un primo pacchetto di raccomandazioni sulle norme tecniche da adottare.

[63] Ente normativo, fondato nel 1961 con sede a Bruxelles, che ha lo scopo di armonizzare e produrre norme tecniche europee, in collaborazione con gli enti normativi nazionali e sovranazionali come l'ISO. Per l'Italia, l'opera di adattamento ed armonizzazione è affidata all'UNI, Ente Nazionale di unificazione.

[64] Comitato Europeo per la normalizzazione elettrotecnica. Fondato nel 1973 a Bruxelles, lavora in stretta collaborazione con l'Unione Europea ed è formato dai vari comitati scientifici a livello nazionale. Per l'Italia si rapporta con il CEI, Comitato Elettrotecnico Italiano. Organismo dal quale vengono promanate le normative EN, standard europei che una volta approvati devono essere adottati senza modifiche in tutti gli Stati membri.

[65] Documento elaborato da CEN-CENELEC Focus Group on Blockchain and Distrbuted Ledger Technologies (FG-BDLT) White Paper Subgroup: N 001, Recommendations for Succesful Adoption in europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies.