Ciberspazio e diritto, vol. 19, n. 61 (3 - 2018), pp. 457-478

I dati personali in ambiente blockchain tra anonimato e pseudonimato

Francesco Rampone*

Sommario: 1. Introduzione. – 2. I dati in ambiente blockchain. – 3. La chiave pubblica. – 4. L'impronta hash. – 5. Coinbase e l'inserimento intenzionale di dati personali in blockchain. – 6. Titolari del trattamento in ambiente blockchain. – 7. Conclusioni.

1. *Introduzione*

Il Regolamento (UE) 2016/679 (GDPR), non diversamente dalla Direttiva 95/46/CE, ha un'impostazione prettamente centralistica, nel senso che esso contempla i trattamenti solo in una dimensione verticale, come operazioni che un soggetto (titolare) compie su dati personali altrui impiegando mezzi propri e scegliendo in autonomia lo scopo del trattamento e le misure di sicurezza adottate avvalendosi, all'occorrenza, di soggetti terzi fornitori di soluzioni informatiche o servizi di *data processing* (responsabili e sub-responsabili).

Al contrario, le soluzioni DLT – *Distributed Ledger Tecnology*, e in particolare la blockchain che di quelle è oggi la massima espressione, hanno uno sviluppo orizzontale, una natura sfuggente che non pare adattarsi alle disposizioni del Regolamento. Forse non tanto per un difetto di quest'ultimo, ma per un limite intrinseco alla architettura decentralizzata del fenomeno in esame, nel senso che una norma, quale essa sia, per sua struttura contempla sempre una condotta o una situazione di fatto o di diritto che permette l'individuazione di un soggetto a cui imputare la responsabilità. Una blockchain, invece, "agisce" per sintesi della volontà

* Avvocato in Milano, esperto in information technology. Capo dipartimento TMT presso La Scala Società tra Avvocati per Azioni. Presidente dell'Associazione Italiana Blockchain.

di una moltitudine indeterminata di soggetti che interagiscono tra loro in modo anonimo e spesso anche inconsapevole del progetto globale a cui ubbidiscono, semplicemente eseguendo le linee di un codice *open source* che opera secondo un protocollo *peer-to-peer* dando origine a quello che qualcuno definisce un vero e proprio organismo[1].

Ebbene, se davvero la tecnologia blockchain è un nuovo Internet[2], se davvero dobbiamo credere che l'interazione decentralizzata tra utenti anonimi darà vita ad un sempre maggior numero di organizzazioni completamente autonome e separate rispetto alla volontà e alla responsabilità dalle persone fisiche che ne sono parte[3], allora dobbiamo interrogarci sulla possibilità che la regolamentazione sulla protezione dei dati personali in ambiente blockchain giungerà presto al suo limite elastico oltre il quale saremo costretti a pensare a questa materia (ed evidentemente a molte altre) in termini completamente nuovi.

[1] Cfr. J. Garzik, "Bitcoin, the organism", «TEDx Talk», Binghamton University, New York, 30 marzo 2014, definisce il bitcoin come un organismo e il suo lavoro di sviluppo come la ricerca di un biologo. Sulla stessa linea di pensiero si pone P. De Filippi, "Blockchain Technology and the Future of Work", «Lift:Lab», Ginevra, 11 febbraio 2016, che paragona le DLT ai *plantoidi*, delle forme di protovita artificiale ideate e realizzate per la prima volta da un team di ricerca dell'IIT (Center for Micro-BioRobotics) di Pontedera. Più recentemente, M. Field, "The Blockchain Revolution: From Organisations to Organism", «TEDx Talk», Breda, 3 novembre 2016.

[2] Cfr. D.&A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World*, Portfolio/Penguin 2016, secondo i quali la bockchain rappresenta la seconda rivoluzione digitale dopo Internet: «*When decentralized blockchain protocols start displacing the centralized web services that dominate the current Internet, we'll start to see real internet-based sovereignty. The future Internet will be decentralized*» (seconda di copertina). Per altri, la blockchain si appresta a riconfigurare Internet in modo completamente nuovo: un Internet 3.0, dall'accesso a pagine statiche (1.0), ai contenuti *user generated* (2.0), alla costruzione di un network disintermediato (3.0). Per una rassegna di *blockchain evangelists*, Cfr. R. Marvin, "Blockchain: The Invisible Technology That's Changing the World", PC Magazine 2017. Available at: https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor.

[3] Attraverso la blockchain si possono costituire delle organizzazioni decentralizzate (DAO – *Decentralized Autonomous Organization*) che hanno regole di governance e operano sul mercato attraverso l'esecuzione di linee di codice (*smart contract*). Essendo prive di organi di amministrazione e controllo e non ricadendo in alcun tipo legale (la natura di tali organizzazioni è molto dibattuta) in quanto sebbene le DAO non schermino dalla responsabilità diretta e illimitata dei loro partecipanti, questi, tuttavia, restano per lo più coperti dall'anonimato (lo stesso network di sviluppatori del protocollo bitcoin, il *BitcoinCore*, è una DAO). Per maggiori dettagli, Cfr. R.C. Merkle, "DAOs, Democracy and Governance", Cryonics Magazine, July-August 2016, Vol. 37:4, pp. 28-40.

Prima di arrivare a tanto, tuttavia, dovremmo chiederci se già oggi l'utilizzo di tecnologie blockchain, nella loro forma pubblica[4], come ad esempio i bitcoin, sia compatibile con le disposizioni del GDPR. Per fare ciò, la prima domanda da porci è se le soluzioni criptografiche basilari impiegate in una blockchain, cioè le chiavi pubbliche e le impronte hash, siano dati personali, e se quindi i nodi di un network *peer-to-peer* debbano rispettare gli adempimenti formali e sostanziali che il Regolamento impone in capo al titolare del trattamento.

2. *I dati in ambiente blockchain*

Sostanzialmente, per funzionare, tutte le blockchain, quale che sia il loro *design*, ricorrono a due soluzioni criptografiche: l'algoritmo RSA e la funzione di hash[5]. Quanto alla prima, abbiamo tutti familiarità con le chiavi asimmetriche poiché sono comunemente utilizzate per le firme

[4] Le blockchain pubbliche (permissionless o aperte) sono quelle dove ciascun utente può di sua iniziativa, senza necessaria accettazione da parte dei partecipanti al network, assumere la funzione di nodo, cioè di operatore che contribuisce al funzionamento del protocollo *peer-to-peer*. Accanto a queste, esistono le blockchain private o semiprivate (permissioned) nelle quali l'ingresso nel network è condizionato alla previa accettazione dei nodi esistenti oppure, benché l'ingresso sia libero, alcuni nodi sono dotati in via esclusiva di privilegi o funzioni particolari (la piattaforma Ethereum, la prima in assoluto per numero di nodi connessi, ha un *design* volto proprio alla realizzazione di blockchain *permissioned* per applicazioni in ambito business).

[5] Il misterioso Satoshi Nakamoto, nel suo articolo apparso in rete nel 2008 (S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008; available at: https://bitcoin.org/bitcoin.pdf) ha descritto tutto il funzionamento dei bitcoin sostanzialmente come una combinazione originale di questi due strumenti matematici. Per approfondire come funzionano i bitcoin e, più in generale, una blockchain, tra le tantissime pubblicazioni suggerisco: A.M. Antonopoulos, *Mastering Bitcoin: programming the open blockchain*, O'Reilly Media 2017; A.M. Antonopoulos, *The internet of money*, Vol. 1 - Vol. 2, Merkle Bloom LLC 2016-2017; D.&A. Tapscott, op cit.. In particolare, per chiarezza e completezza di esposizione, segnalo J-L. Verhelst, *Bitcoin, the blockchain and beyond: a 360-degree onboarding guide to the first cryptocurrency and blockchain*, Amazon Digital Services 2017; A. Wright, *Blockchain: uncovering blockchain technology, cryptocurrencies, bitcoin and the future of money*, Amazon Digital Services 2017; J.B. Morley, *That Book on Blockchain: A One-Hour Intro*, Amazon Digital Services 2017. Più in generale sul fenomeno peer-to-peer, ancorché datato, è ancora attuale, visionario e ricco di spunti di riflessione il florilegio a cura di A. Oram, *Peer-to-peer: Harnessing the benefits of a disruptive technology*, O'Reilly Media 2001.

digitali e la posta elettronica certificata (PEC). Le chiavi altro non sono che due sequenze di numeri e lettere generate in coppia la cui caratteristica consiste nel fatto che il testo cifrato con una di esse può essere decifrato solo con l'altra. Ciò comporta che pubblicando una delle due chiavi (la c.d. chiave pubblica) dichiarando al tempo stesso di essere in possesso dell'altra (la c.d. chiave privata), ma tenendola segreta, si può dimostrare la provenienza e quindi la paternità di un messaggio. Se infatti questo può essere decifrato con una determinata chiave pubblica, vorrà dire che solo colui che si è dichiarato possessore della corrispondente chiave privata (e solo lui) lo ha originariamente criptato.

Quanto alla funzione di hash, essa è un algoritmo matematico che consente di trasformare un testo di lunghezza arbitraria in una sequenza di numeri e lettere di lunghezza definita sempre uguale, e che, al variare anche minimo dell'input (il testo sottoposto a cifratura) corrisponde un output completamente diverso (testo cifrato). Tale caratteristica consente di creare un'impronta del testo, giustappunto detta *impronta hash* o *digest*, che tuttavia non contiene abbastanza informazioni per poter essere riconvertita nel testo originario poiché, come detto, l'output ha lunghezza predefinita e quindi, benché abbia un'enorme variabilità[6], corrisponde ad un numero finito di permutazioni a fronte di un numero infinito di possibili input. Questo è ciò che i matematici chiamano unidirezionalità della funzione.

A questo punto la domanda è: la chiave pubblica e l'impronta di hash, come utilizzati tipicamente in blockchain, possono considerarsi *dati personali*? E se così, in quali condizioni?

Va detto che esistono diverse blockchain, alcune provviste di un'architettura studiata proprio allo scopo di tutelare la privacy degli utenti pur garantendo efficienza e decentralizzazione[7]. Si tratta tuttavia di

[6] Ad esempio, nella blockchain dei bitcoin si fa uso della funzione SHA256 che genera una stringa alfanumerica di 64 caratteri (32 bit), né più né meno, per un totale di diverse combinazioni pari a circa 2 elevato a potenza 256, un numero che compete con quello degli atomi nell'Universo osservabile.

[7] Esistono criptovalute, come per esempio Dash, Z-Cash o Monero, che adottano soluzioni molto sofisticate per garantire la non tracciabilità delle transazioni. Per un'esaustiva disamina delle tecniche e misure oggi disponibili per proteggere la *privacy* in blockchain (cioè per ostacolare con soluzioni criptografiche e logiche la rintracciabilità delle persone fisiche che hanno effettuato le transazioni) è ancora attuale ciò che ha scritto un paio di anni fa il fondatore di Ethereum, Cfr. V. Buterin, "Priva-

soluzioni che destano poco interesse nel giurista poiché non entrano nel merito della natura dei dati trattati, ma si preoccupano solo di elevare ai massimi livelli la loro riservatezza e pretendono di legittimare alla radice il trattamento semplicemente (si fa per dire) adottando sofisticate tecniche criptografiche.

3. *La chiave pubblica*

Tra i primi commentatori che hanno studiato le implicazioni della tecnologia blockchain in una prospettiva privacy e GDPR c'è chi sostiene che le chiavi pubbliche siano senza eccezioni dati pseudonimi[8], se non addirittura dati personali[9]. Ritengo tali conclusioni in parte errate e dettate dalla supposta relazione esistente tra chiave pubblica e identità personale del titolare della corrispondente chiave privata. Conclusione probabilmente indotta in parte dal comune utilizzo che si fa delle chiavi pubbliche nell'ambito dei servizi di posta certificata e firma digitale dove

cy on the Blockchain", 2016. Available at: https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/.

[8] Cfr. R.R. Kumar, "Impact of Blockchain Technology on Data Protection and Privacy" 17 luglio 2017, available at SSRN: https://ssrn.com/abstract=3040969 or http://dx.doi.org/10.2139/ssrn.3040969; P. De Filippi, "The interplay between decentralization and privacy: the case of blockchain technologies", «Journal of Peer Production, Issue n.7: Alternative Internets» 2016, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689; S. Ramsay, "The General Data Protection Regulation vs. The Blockchain - A legal study on the compatibility between blockchain technology and the GDPR", Thesis in Law and Informatics, Stockholm University 2016, available at: http://www.diva-portal.se/smash/get/diva2:1221579/FULLTEXT01.pdf. In ambito nazionale, Cfr. R. Bocchini, "Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche", «Rivista di Diritto Industriale», vol. I, 2017, pp. 48 ss.; L. Piatti, "Dal codice civile al codice binario: *blockchain* e *smart contracts*", «Ciberspazio e diritto», vol. 17, n. 56, p. 327, nota 7. Questi ultimi Autori in realtà non qualificano i bitcoin come dati pseudonimi con specifico riferimento alla normativa privacy, ma si limitano a rilevare il fatto che tali dati possono, con le opportune associazioni ad altre informazioni, rivelare un'identità personale. Cosa vera ovviamente, ma applicabile a qualsiasi informazione e quindi irrilevante per discriminare tra dati personali e anonimi ai sensi del GDPR.

[9] Cfr. M. Finck, "Blockchain and Data Protection in European Union", «Max Planck Institute for Innovation & Competition Research» Paper No. 18-01, feb. 2018. Available at SSRN: https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3080322.

sono impiegate proprio a fini identificativi del soggetto che dispone della chiave privata[10].

Ebbene, poiché l'equazione chiave pubblica=dato pseudonimo condiziona in modo decisivo ogni ulteriore riflessione in materia, con il presente contributo intendo dimostrare non solo che ciò non è sempre vero, ma che non è affatto vero in condizioni normali, cioè nelle condizioni in cui le chiavi pubbliche sono impiegate dagli utenti e dai nodi in un protocollo blockchain.

Va innanzi tutto sottolineato che una chiave pubblica è utilizzata in blockchain senza dichiarare apertamente il soggetto utilizzatore della corrispondente chiave privata (a meno che lui stesso non lo disideri). Una chiave pubblica, inoltre, non sempre è associata all'indirizzo di una persona fisica in quanto potrebbe essere utilizzata anche da una persona giuridica. D'altra parte, potrebbe anche essere utilizzata per identificare non una persona, fisica o giuridica, ma addirittura un oggetto inserendo la chiave privata in un tag e gestendo la corrispondente chiave pubblica in blockchain per tracciare una filiera produttiva[11]. È pertanto escluso che l'equazione chiave pubblica=dato personale sia sempre corretta potendo la chiave rappresentare in blockchain un ente giuridico o una cosa.

Ma anche allorché la coppia di chiavi sia utilizzata da una persona fisica, tale equivalenza assoluta si dimostra fallace in quanto siamo al di fuori di un uso *a fini identificativi* come invece avviene con la chiave pubblica di un account di PEC o di un sistema di firma digitale. In questi casi

[10] Negli stessi termini di stretta relazione tra chiave pubblica e identità del titolare dell'indirizzo bitcoin ha ragionato anche il Consiglio Nazionale del Notariato in risposta ad un quesito (Quesito Antiriciclaggio n. 3-2018/B) in cui si chiedeva se il pagamento del prezzo della vendita di un bene immobile in bitcoin violi le norme in materia di limitazione all'uso del denaro contante e quelle in materia di indicazione analitica dei mezzi di pagamento. Sul punto mi permetto di rinviare ad una mia nota critica, "Compro casa e pago in bitcoin: perché il parere del Notariato non convince del tutto". Available at Iusletter.com: http://iusletter.com/compro-casa-pago-bitcoin-perche-parere-del-notariato-non-convince-del/.

[11] L'utilizzo di tecnologia *secured element* e HCE – *Host Card Emulation* in combinazione con la blockchain promette nel prossimo futuro di rivoluzionare non solo la filiera produttiva e distributiva, ma ogni aspetto della nostra vita (per un'interessante applicazione sviluppata da IBM e Walmart, "Genius of Things: Blockchain and Food Safety with IBM and Walmart", 2017. Available at: https://www.youtube.com/watch?v=MMOF0G_2H0A). Altri progetti interessanti di applicazione della blockchain in questo settore sono Provenance (tracciabilità di prodotti di consumo), Skuchain (filiera industriale non food) e Blockverify (prodotti lusso).

la chiave pubblica serve proprio all'identificazione del titolare della chiave privata in quanto ciò è necessario per attribuire ad esso la possibilità di attestare la paternità di documenti in modo certo e univoco in un atto di comunicazione digitale. In una blockchain, al contrario, chiunque può effettuare una transazione senza che nel network sia attribuita un'identità al debitore o al creditore. Solo ricorrendo a potenti mezzi di *digital forensic* e *big data analysis* nonché facendo presunzioni (es.: corrispondenza tra indirizzo IP e utente), avendo accesso a informazioni riservate disponibili solo dietro ordine di autorità (es.: tabulati dell'Internet provider) o utilizzando comuni mezzi di indagine (es.: rintracci di spedizioni), si può risalire all'identità delle parti di una transazione in blockchain. Ma siamo nell'ambito di casi eccezionali e non sempre efficaci, al di fuori dei quali la chiave privata non consente in sé alcuna identificazione e non ricade quindi nella definizione di *dato personale*.

A questo punto è utile rileggere i chiarimenti forniti nell'ancora attualissimo parere n. 4 del 20 giugno 2007 (WP136) del Gruppo di Lavoro *ex* articolo 29 (art. 29 della Direttiva 95/46/CE – Working Party) dove sono indicati dettagliati criteri interpretativi per verificare se un dato possa o meno qualificarsi come *personale*.

Partendo dalla definizione di dato personale fornita dalla direttiva 95/46/EC («any information relating to an identified or identifiable natural person»[12]), e dopo aver fornito un chiarimento sulla nozione di «information», per cui sostanzialmente tutto è informazione, il Working Party si sofferma sulla relazione tra informazione e persona fisica e cioè sul significato dell'espressione «relating to»[13] e propone un test articolato su tre verifiche: *contenuto*, *scopo* e *risultato*. Secondo tale test un'informa-

[12] La definizione è mutata dall'art. 2 della Convenzione di Strasburgo del 1981 *sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale* che già definiva dato personale «any information relating to an identified or identifiable individual». Così anche nella Direttiva (art. 2) e nel Regolamento (art. 4) con l'unica sostituzione di «individual» con «natural person».

[13] Da notare che nella traduzione italiana della Direttiva e del Regolamento il dato personale è «*qualsiasi informazione* concernente *una persona fisica identificata o identificabile*» (Direttiva e Convenzione) e «*qualsiasi informazione* riguardante *una persona fisica identificata o identificabile*» (Regolamento). Aver tradotto *relating to* con gli aggettivi *concernente* e *riguardante* rischia di modificare il senso originario della disposizione in senso restrittivo (anche se va riconosciuto che un passo avanti è stato fatto con il Regolamento). Se infatti il numero di previdenza sociale *concerne* un individuo, la targa di un mezzo pubblico no, né propriamente lo riguarda, ma può ciò nondimeno in determinate circo-

zione è riferita ad una persona fisica qualora il trattamento abbia come *contenuto* dati direttamente riferibili ad un individuo, come la foto di una persona o la sua cartella clinica; oppure dati non riferibili ad un individuo, ma il cui trattamento abbia lo *scopo* di identificare una persona fisica, come i dati di un sistema di videosorveglianza che vengono conservati per un certo periodo proprio per risalire in caso di commissione di atti illeciti all'identificazione dell'autore del reato; oppure dati il cui trattamento, ancorché non indirizzato all'identificazione di una persona fisica, abbia come *risultato* tale identificazione, come la geolocalizzazione di un parco macchine di servizio taxi per ottimizzare le chiamate che si risolve in un monitoraggio degli spostamenti dei tassisti.

Ancorché il test conduca, almeno sotto il profilo della relazione tra dato ed individuo, ad una definizione amplissima di dato personale (anche perché i tre elementi non devono ricorrere cumulativamente, ma anche solo alternativamente), esso produce un risultato negativo quando applicato alle chiavi pubbliche non identificative, ovvero nel modo in cui sono generalmente utilizzate in una blockchain.

Quanto al *contenuto*, vien da sé che una chiave pubblica non è un dato personale di immediata percezione come tale; quanto allo *scopo*, è altrettanto evidente che il trattamento della chiava pubblica non è effettuato per identificare i possessori della chiave privata, né nasce con questo scopo, ma è impiegata al solo fine tecnico di consentire una transazione offrendo una soluzione al problema della *double spending*[14]. Infine, quanto al *risultato*, è pur vero che in taluni casi la chiave pubblica può ricondurre alla identificazione di un individuo, ma ciò è dovuto all'utilizzo di altri dati e metadati che in combinazione tra loro consentono a posteriori di qualificare la chiave come elemento identificativo di una transazione compiuta da un determinato individuo, il che non equivale a dire che la chiave sia di per sé un dato personale[15].

stanze essere *associata* ad un individuo – e in tal senso anch'essa costituisce dato personale – consentendo di risalire *per relazionem* ai dati personali di un individuo determinato.

[14] Cfr. S. Nakamoto, op. cit., § 2 (*Transactions*). Senza l'impiego della criptografia asimmetrica sarebbe impossibile impedire ad un utente la spendita di una stessa moneta virtuale per effettuare pagamenti multipli facendo venire meno la fiducia nel sistema. Allo stesso modo, tutti i progetti di blockchain utilizzano le chiavi pubbliche per creare fiducia in una rete priva di gerarchie (*trustless*).

[15] Lo stesso inventore dei bitcoin, S. Nakamoto, op. cit., ha chiarito che il network garantisce la privacy poiché le chiavi pubbliche sono utilizzate in modo anonimo

Per comprendere meglio questo ultimo aspetto è utile menzionare il caso Cooper-Alba. Nel luglio 2013, il famoso attore Bradley Cooper usciva da un albergo di New York e veniva fotografato mentre prendeva un taxi di cui era riconoscibile la targa. A marzo di quello stesso anno, un cittadino americano, invocando la Freedom of Information Law dello stato di New York, chiedeva alla *Taxi and Limousine Commission* della città il rilascio del database contenente tutte le corse dei taxi (circa 173 milioni) con indicazione del tragitto effettuato, della tariffa pagata e delle eventuali mance date al conducente. Ben presto quel database fu messo in rete e non ci volle molto perché i fan dell'attore incrociando i dati della fotografia (la targa o la sigla del taxi) con quelli del database, scoprissero non solo dove era stato Cooper, ma anche se e quanto aveva lasciato di mancia. La stessa indagine è stata poi replicata per innumerevoli vip (spesso paparazzati nel momento in cui erano allo scoperto, ovvero proprio nell'atto di prendere un taxi), tra cui Jessica Alba, rinvenendo vecchie fotografie pubblicate su tabloid di tutto il mondo e scoprendo così le loro destinazioni e abitudini.

Nel caso appena citato, la targa o la sigla dei taxi non sono dati personali in sé; non identificano affatto l'attore Cooper (lo fa la foto del paparazzo). Un taxi può essere utilizzato da chiunque per andare da un luogo ad un altro e manca quindi quel collegamento univoco *individuo-codice* che farebbe della targa un dato – per l'appunto – personale (pseudonimo). Allo stesso modo, anche una chiave pubblica non è un dato personale. Infatti, proprio come la targa del taxi essa non identifica di per sé un individuo trattandosi, come già accennato, solo di un mezzo tecnico per compiere o ricevere un pagamento su una rete telematica.

Peraltro, per sottolineare quanto sia effimero il legame tra chiave pubblica e identità personale, si pensi al fatto che un individuo può generare e utilizzare una diversa coppia di chiavi criptografiche per ogni tran-

separando le identità degli operatori dalle transazioni che compiono, come accade in borsa dove si conosce il volume degli scambi, ma non l'identità di chi compra le azioni (ivi, § 10, 6). Questa sembra anche essere l'opinione della BCE: «VC payment transactions do not require the provision of personal or sensitive data, unlike credit card data or passwords in the case of conventional payment methods. In this sense, VC units can be considered to be like cash: whoever possesses them also owns them, removing a source of potential identity», EBA "Opinion on 'virtual currencies'" del 4 luglio 2014 (EBA/Op/2014/08).

sazione[16], oppure può effettuare la transazione anche passando la chiave privata "di mano in mano" come atto di soluzione del pagamento. Una transazione, infatti, può avvenire anche *off line* con la consegna di un token nel quale sono caricate le chiavi private che danno accesso agli indirizzi in blockchain. Sono già in circolazione delle "monete" che funzionano in questo modo[17], e se anche non avranno un grande successo, esse dimostrano che una chiave pubblica, almeno in principio, non è un dato personale più di quanto lo sia il numero di serie stampato sulla facciata delle banconote che portiamo in tasca[18].

Alla luce di quanto precede, il test di *risultato* sull'espressione «relating to» va condotto in termini restrittivi, nel senso che non basta che un dato per essere considerato personale sia utile in qualche modo al rintraccio di informazioni che riguardano un individuo, bisognerebbe altrimenti ammettere che qualsiasi dato, anche il tempo atmosferico, è dato personale[19].

[16] Questo è già possibile farlo con i bitcoin generando nuove coppie di chiavi per ogni transazione (già S. Nakamoto, op. cit., 6) oppure unendo le transazioni di più utenti in una sola, come fa il sistema CoinJoin, impedendo alle società di *blockchain analytics* di risalire ai titolari di *wallet*.

[17] L'esempio più noto di bitcoin fisici è Casascius (https://www.casascius.com/). Si tratta di supporti metallici a forma di moneta su cui la chiave pubblica è visibile (per verificare il credito), ma la chiave privata è nascosta da un adesivo olografico che viene distrutto se rimosso. L'integrità dell'adesivo è quindi garanzia del valore facciale della moneta.

[18] Cfr. R. Bocchini, op. cit., 51, il quale scrive: «Solamente il contante è veramente anonimo, visto che il possesso vale titolo e quindi non vi è alcuna registrazione in merito al cambiamento di proprietà». Ma anche per le criptovalute il possesso vale titolo, solo che il possesso non ha ad oggetto la banconota fisica, ma le chiavi private. Peraltro, anche il denaro contante si comporta esattamente come le criptovalute, Per esempio, nell'ambito di indagini per reati di riciclaggio, traffico di stupefacenti, corruzione e concussione, non è raro che si tenga traccia dei numeri di serie delle banconote così da acquisire la prova della condotta illecita. In tali casi, il passaggio di mano delle banconote comporta un trattamento di dati personali, quelli dell'*accipiens* non diversamente da quanto accadrebbe con le criptovalute. Anzi, nel caso delle comuni banconote, si verifica un momento identificativo certo, ovvero quello della dazione in cui la persona fisica materialmente consegue il possesso del denaro. Con le criptovalute, invece, neanche questo è vero potendo l'*accipiens* limitarsi ad indicare un indirizzo (anonimo) su cui fare l'accredito e immediatamente dopo "ripulire" il denaro con innumerevoli pagamenti a sé o a terzi in buona fede facendo così perdere le tracce dell'origine illecita dei proventi.

[19] Cfr. N. Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law", «Law, innovation, and technology», 10(1), 2017, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355, la

Veniamo ora all'ultima parte della definizione, «identified or identifiable». Qui l'intento del legislatore è chiaro, non è dato personale solo quello direttamente identificativo, ma lo è anche il dato che può essere messo in relazione, direttamente o indirettamente, a dati personali contenuti in una *lista di corrispondenza*. Ciò significa che il collegamento logico tra dato e individuo può essere anche solo potenziale o addirittura manifestarsi in un momento successivo al primo atto di trattamento, sicché il dato non è *personale* al momento della raccolta, ma diventa tale per effetto dell'avanzamento tecnologico o del mutamento delle condizioni di fatto o di diritto di colui che lo tratta. E così una chiave pubblica, che di per sé non è informazione identificativa – esattamente come non lo è la targa di un taxi –, non "nasce" come dato personale, ma lo diventa solo il momento in cui sia eventualmente utilizzata in associazione con altre informazioni (es.: utenza telefonica, indirizzo IP o la foto del taxi nell'esempio fatto) che invece identificative sono (o sono collegate a loro volta ad identificatori)[20].

Ma il concetto di identificabilità va ristretto, nel senso che non tutto ciò che è possibile va preso in considerazione. Verrebbe altrimenti da dire che ciò che, correttamente, non si è qualificato come dato personale interpretando in modo restrittivo l'espressione «relating to», rischi di esserlo adottando un'ampia accezione di «indetifiable». Torneremmo quindi a concludere che qualsiasi informazione, poiché utile anche solo in astratto all'identificazione di un individuo e quindi suscettibile di essere intesa alla stregua di un dato pseudonimo, sia soggetta al GDPR[21].

quale, richiamando i lavori di P. Ohm ("Broken Promises of Privacy", «UCLA Law Rev.», vol. 57, 2010, pp. 1742 ss.), L. Sweeney ("Simple demographics often identify people uniquely", 2000, available at: https://dataprivacylab.org/projects/identifiability/paper1.pdf) e P. Schwartz, D. Solove ("The PII Problem: Privacy and a New Concept of Personally Identifiable Information", «New York Univerisity Law Quarterly Rev.», vol. 86, 2011, p. 1876), ritiene che il tasso di sviluppo tecnologico e la mole sempre più ampia di dati a disposizione per analisi di Big Data renda l'anonimato assoluto irrealizzabile e (per l'esempio del tempo atmosferico, *ivi*, § 3.5, p. 16).

[20] *Ivi*, p. 5: «The same piece of data can be anonymous at the time of collection, but turn into personal later, just sitting there, simply by virtue of technological progress».

[21] Il rischio è avvertito da O. Tene & J. Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics", «Northwestern Journal of Technology and Intellectual Property», vol. 11, 2013, p. 258: «with a vastly expanded definition of PII, the privacy framework would become all but unworkable […] anonymized information always carries some risk of re-identification, many of the most pressing privacy risks

In un approccio meno assolutista, invece, l'identificabilità di un individuo va intesa in relazione alle circostanze concrete, cioè tenendo in considerazione il diverso grado di possibilità tecnica, giuridica o di fatto di avere accesso alle informazioni che consentono tale identificabilità[22].

Venendo alla chiave pubblica, va riconosciuto che sebbene sia possibile in talune circostanze risalire all'identità del titolare della chiave privata, si tratta di circostanze straordinarie che richiedono l'impiego di mezzi e risorse non comuni, e qualche volta non leciti. Non esiste infatti una lista di corrispondenza "chiave pubblica-titolare chiave privata", né tale corrispondenza è ottenibile nelle normali circostanze in cui la chiave pubblica è impiegata in una blockchain. La chiave pubblica, insomma, è solo un frammento di informazione che indica una certa disponibilità di credito (o altro diritto) ad una certa data, ma che non dice a chi spetta tale credito. Allo stesso modo di come la targa del taxi, nel caso Cooper-Alba, è solo un frammento di informazione che di per sé non costituisce dato personale, ma che in combinazione ad altre informazioni (foto e database) potrebbe consentire in circostanze eccezionali di risalire ad un individuo e ai dati personali che lo riguardano, ovvero la sua destinazione in un dato giorno e la sua propensione a pagare mance.

Sulla scia della sentenza CGUE nel caso *Breyer*[23], si potrebbe essere tentati di considerare la chiave pubblica alla stregua di un indirizzo IP dinamico[24]. In entrambi i casi, infatti, si tratta di un codice associato ad una singola operazione (la transazione nel caso della blockchain, la sessione di accesso nel caso della navigazione in rete). A ben vedere, tuttavia, si può cogliere una differenza. Innanzi tutto, nel caso sottoposto alla Cor-

exist only if there is reasonable likelihood of re-identification […] many beneficial uses of data would be severely curtailed if information, ostensibly not about individuals, comes under full remit of privacy laws based on a remote possibility of being linked to an individual at some point in time through some conceivable method, no matter how unlikely to be used».

[22] Cfr. P.M. Schwartz, D. Solove, op. cit., p. 1876: «Different levels of effort will be required to identify information, and varying risks are associated with the possible identification of data. To place all such data into the same conceptual category as data that currently relate to an identified person is a blunt approach».

[23] Cfr. sentenza CGUE (Seconda Sezione) del 19 ottobre 2016, Patrick Breyer/Bundesrepublik Deutschland (Causa C-582/14). Secondo la Corte, accogliendo l'interpretazione di «identifiable» fatta propria anche dal WP136 nell'esempio n. 15, l'indirizzo IP dinamico è un dato personale.

[24] Così ritiene M. Finck, op. cit., p. 13.

te, l'indirizzo dinamico era trattato proprio allo scopo di risalire in futuro all'identità di colui che aveva avuto accesso al sito, e ciò è sufficiente per non superare il test WP136 nella parte del «relating to» (§ 2 del WP136). La chiave pubblica, invece, non è trattata in blockchain per tale scopo, ma solo per conseguire l'effetto tecnico di eseguire una transazione risolvendo, come già accennato, il problema del *double spending*. Ma c'è un'altra differenza decisiva, e cioè che l'indirizzo IP dinamico utilizzato da un terminale in una determinata sessione è *stabilmente associato* ad all'identità dell'utente che ha sottoscritto il contratto con l'ISP. Quest'ultimo, pertanto, è in possesso di una lista di corrispondenza che consente in modo stabile e duraturo di risalire all'identità di chi ha avuto accesso al sito. L'IP dinamico, quindi, ricade sotto la definizione di dato personale del WP136 anche sotto il profilo dell'identificabilità dell'individuo (§ 3 del WP136). Lo stesso non accade per le chiavi pubbliche utilizzate in blockchain per le quali non esiste una tale lista di corrispondenza, e anche laddove ci fosse un'occasionale corrispondenza tra chiave e identità personale, come ovviamente accade nel caso di un pagamento in cui il debitore e il creditore si conoscono l'un l'atro, si tratterebbe per lo più di una corrispondenza contingente alla transazione in corso e non estendibile ad altre. Siamo però nell'ambito di casi particolari che non soddisfano il limite interpretativo di *identificabilità*.

In conclusione, il concetto di «*identificabile*», utilizzato nella definizione de dato personale, va inteso in relazione agli strumenti che possono essere «ragionevolmente utilizzati»[25]. Non quindi un'identificabilità in astratto, ma in concreto, calata cioè nelle mutevoli circostanze oggettive e soggettive di chi tratta il dato: «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» (considerando n. 26 del GDPR).

[25] Così specifica il considerando n. 26 della direttiva 95/46/CE e, in termini analoghi, lo stesso considerando nel GDPR.

4. *L'impronta hash*

Come visto (par. 2), la funzione hash è utilizzata ampiamente nel protocollo blockchain per sintetizzare in una stringa alfanumerica univoca (quasi-univoca) un set di informazioni che, a loro volta, possono riferirsi a transazioni (cioè costituzione, modificazione o estinzione di diritti), beni (materiali e immateriali) o persone (fisiche o giuridiche). Ad esempio, in un servizio di gestione IPRs non sempre un'opera dell'ingegno potrebbe essere oggetto di transazioni in blockchain se fosse caricata in rete tal quale. Problemi di dimensione del file ne ostacolerebbero la circolazione tra nodi impendendo il formarsi di consenso tra loro. I nodi, in sostanza, non potrebbero accettare la transazione in un blocco perché troppo voluminosa o comunque la rifiuterebbero perché renderebbe il blocco poco remunerativo[26]. Infatti, ancorché la blockchain sia spesso definita come un database decentralizzato, essa è più un libro mastro, cioè un *registro decentralizzato*, costruito non tanto per archiviare informazioni, ma per annotare transazioni in blocchi di dimensione relativamente contenuta (un megabyte nel protocollo bitcoin). Per questo motivo le transazioni non avrebbero ad oggetto voluminosi file, ma un'impronta hash che, con pochi caratteri[27], può identificare l'opera in modo univoco e oggettivo fornendo una prova inconfutabile della sua esistenza e dello scambio avvenuto.

Secondo il WP136, le funzioni unidirezionali, qual è la funzione hash, generano degli output che, proprio in forza di tale unidirezionalità, e cioè al fatto che non esiste un modo per ricavare il dato originario conoscendo solo l'hash, non posso considerarsi dati personali, ma dati anonimi a tutti gli effetti (WP136, pp. 18 e 20)[28].

[26] Per ciascuna transazione contenuta in un blocco, il nodo che lo aggiunge in blockchain viene remunerato con delle *transaction fee*. Più transazioni contiene il blocco, più sono le *transaction fee* che il nodo conta di ottenere (Cfr. A.M. Antonopoulos, *Mastering Bitcoin*, cit., § 4).

[27] Nei bitcoin è utilizzata la funzione SHA256 il cui hash è lungo 256 bits, equivalente a 64 bytes (caratteri) in formato esadecimale.

[28] Pur richiamando lo stesso passaggio del WP136, M. Finck, op. cit., p. 11, erroneamente attribuisce al Working Party una conclusione diversa, ovvero che l'impronta hash è un dato pseudonimo, e poiché tale Autore ritiene che un dato pseudonimo debba invariabilmente considerarsi dato personale, conclude che un'impronta hash è un dato personale.

L'affermazione del Working Party non è però perentoria («la crittografia unidirezionale […] crea *in genere* dati anonimi», enfasi aggiunta). L'organismo fa evidentemente riferimento ai *key-coded data*, cioè ai dati personali codificati con una chiave univoca il cui trattamento equivale al trattamento dei dati codificati (WP136, p. 18). A poco rileva infatti se il codice sia stato attribuito con una funzione unidirezionale o con un processo casuale. L'intento del legislatore qui è evidente: mascherare i dati personali con un codice univoco non consente di evitare per ciò solo le prescrizioni della legge nella misura in cui il soggetto a cui i codici si riferiscono sia in qualche modo *identificabile* (che quindi, come visto, esista una lista di corrispondenza e sia ragionevolmente accessibile).

È quindi proprio sul significato di *identificabilità*, ancora una volta, che occorre porre l'accento. Come visto, il Working Party in proposito accoglie una nozione dinamica, nel senso di considerare l'identificabilità non in senso oggettivo, come possibilità astratta riconosciuta in modo indipendente da colui che tratta il dato, ma in senso soggettivo, cioè come possibilità che in concreto ha un determinato soggetto di risalire all'identità di un individuo. In tale prospettiva, quindi, un *key-coded data* non deve sempre essere inteso come dato personale perdendo questa qualifica quando esso costituisca (nel caso concreto) effettivo ostacolo alla reidentificazione del soggetto interessato, ovvero non sia *ragionevolmente probabile* che siano affrontati i costi e impiegati i mezzi necessari a tale scopo.

Se quindi adottiamo, come dobbiamo, una nozione relativa e soggettiva di *identificabilità*, per proprietà transitiva dobbiamo fare altrettanto per la definizione di dato personale che a quella nozione rinvia[29]. I *key-coded data*, allora, sono dati personali solo per il possessore della lista di corrispondenza tra codici e identità del soggetto interessato e per coloro che ragionevolmente possono entrarne in possesso, ma non lo sono per tutti coloro che, pur trattando i medesimi dati, quella lista non hanno e non è consentito loro (ed anzi è impedito con adeguati mezzi) avere[30].

[29] L. Putrova, op. cit., p. 7.

[30] Sul punto si veda WP136, esempio n. 17, e, in particolare, laddove il Gruppo di lavoro, con riferimento ai *key-coded data* trattati da terzi chiarisce: «In questo caso, si può concludere che i dati codificati con chiave costituiscono informazioni concernenti persone fisiche identificabili per tutte le parti eventualmente coinvolte nell'identificazione, e vanno sottoposti alle norme di protezione dei dati. Questo non significa tuttavia

Non si può quindi dire a priori se una stringa hash sia un dato personale. Ciò dipende dalle circostanze di fatto in cui si trova chi compie il trattamento dovendosi verificare quale diritto, quali mezzi e quali possibilità egli abbia in concreto di risalire alla lista di corrispondenza e, quindi, all'identità del soggetto interessato.

Ebbene, nell'uso dei codici hash in blockchain, come per le chiavi pubbliche, tale lista non esiste, né è necessaria, né i codici hash sono utilizzati per risalire in qualche modo all'identità di un individuo, né sono impiegati per camuffare l'identità di un soggetto interessato. Nel protocollo bitcoin, ad esempio, le funzioni hash (SHA256) sono utilizzate per fare il *digest* delle chiavi pubbliche, assegnare un'impronta a ciascuna transazione e un'impronta all'insieme delle impronte contenute in un blocco (*Merkle tree*) per creare l'intestazione del blocco stesso, anch'esso a sua volta cifrato con la medesima funzione per ottenere un'impronta che sarà elemento costitutivo dell'intestazione del blocco successivo. Proprio come le chiavi pubbliche, anche in questo caso il codice hash non supererebbe il test del WP136 difettando contenuto, scopo e risultato.

Ma oltre alle blockchain per gestire criptovalute, potrebbero esserci blockchain progettate per gestire un altro genere di dati, come nell'esempio accennato di *IP management*[31] o di network per la fornitura di servizi governativi attraverso identità digitale[32], o di condivisione dati e gestione ciclo vita di apparecchi nel mondo IoT. In tali casi, non è esclu-

che altri responsabili del trattamento che stiano lavorando sugli stessi dati codificati stiano effettivamente trattando dati personali se il regime specifico nel quale questi altri responsabili operano esclude esplicitamente la reidentificazione e sono state adottate misure tecniche adeguate al riguardo» (enfasi aggiunta). Quanto alle misure tecniche citate, esistono oggi soluzioni criptografiche assai sofisticate per cui uno *smart contract* potrebbe processare dati personali e restituire l'output voluto pur senza consentire l'accesso a tali dati o al modo in cui sono stati trattati (vedi le soluzioni *zero knowledge proof* e *black box*, descritte da V. Buterin, cit.).

[31] Per la gestione di diritti d'autore segnalo i progetti Mycelia e Ujo Music il cui stato di avanzamento non è tuttavia chiaro. Ma i settori in cui si sta sperimentando la tecnologia blockchain sono innumerevoli e vanno dal retail (OpenBazar e OB1), alle assicurazioni (Aeternity), dal data storage (Storj) alla sanità (Gem e Tieron) per finire nell' immobiliare (Ubiquity).

[32] Il caso più avanzato al mondo di applicazione blockchain in servizi ai cittadini è quello della Repubblica d'Estonia che con il suo ID-kaarts sta portando avanti con ottimi risultati un progetto nazionale denominato *Zero-Bureaucracy* (https://www.mkm.ee/en/zero-bureaucracy). Successo tanto più rimarchevole se si pensa che il Paese fino al 1991 ha fatto parte del dissolto blocco sovietico, come noto di stampo assai centralista.

so che un'impronta hash possa essere utilizzata proprio per compiere un trattamento più o meno diretto di dati personali. Se per esempio in un network blockchain fossero trattate le impronte hash della chiave pubblica di una firma digitale, quelle impronte sarebbero a tutti gli effetti dati personali poiché esisterebbe una lista di corrispondenza accessibile a tutti tra chiave pubblica e identità del detentore della chiave privata. E ancora, se l'impronta hash fosse ottenuta per esempio cifrando un codice fiscale, anche in questo caso l'impronta sarebbe un dato personale in quanto, benché non esista una lista di corrispondenza pubblica tra identità e codice fiscale, è noto l'algoritmo per ricavare dai dati personali della prima (nome, cognome, data e luogo di nascita) il secondo, almeno nella grande maggioranza dei casi[33]. In entrambi gli esempi citati, comunque, non solo la lista di corrispondenza dovrebbe essere nota (o facilmente ricavabile come nel caso dei codici fiscali), ma dovrebbe essere noto anche il protocollo di codifica applicato alla funzione hash. Dovrebbe cioè essere noto che le impronte sono state ottenute codificando le chiavi pubbliche della firma digitale o i codici fiscali. Sicché ottenuta l'impronta hash della chiave pubblica o del codice fiscale di un individuo, basterebbe interrogare la blockchain e cercare le corrispondenze per conoscere i dati personali riguardanti quell'individuo e caricati in blockchain.

Ma se il protocollo di codifica fosse noto solo al titolare originario dei dati e non fosse così banale come negli esempi appena fatti, allora l'impronta hash potrebbe essere utilizzata per gestire in blockchain informazioni anche di carattere personale senza per ciò qualificarsi come trattamento di dati personali. In tal caso, infatti, solo il titolare dei dati avrebbe accesso alle informazioni necessarie per la *reidentificazione* delle impronte (protocollo di codifica o lista di corrispondenza)[34].

[33] In questo caso, si tratterebbe di una verifica a posteriori: dal *digest* non si può ricavare il codice fiscale, ma si può verificare se il *digest* è ottenuto da un determinato codice fiscale. È quindi possibile verificare il riferimento ad un'identità specifica. In L. Sweeney, op. cit., § 2.1, l'Autore dimostra come abbia potuto reidentificare migliaia di individui incrociando i loro dati sanitari "anonimi" fornitigli dalla *National Association of Health Data Organizations* (NAHDO) con i dati della lista dei votanti della cittadina di Cambridge in Massachussets. Ha così potuto associare dati sensibili di pazienti identificati solo con il codice postale, la data di nascita e il sesso con il loro nome, indirizzo e fede politica.

[34] Non è certo che basti aggiungere un po' di "sale" al protocollo di codifica per scongiurare il trattamento di dati personali H. Chang, "Is Distributed Ledger Technology Built for Personal Data?", «Journal of Data Protection & Privacy», vol. 1, n. 4, 2018, pp. 5-6. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137606.

Concludendo, anche per l'impronta hash vale quanto detto a proposito della chiave pubblica, e cioè che essa di per sé non costituisce dato personale, come peraltro, forse con eccessiva generalizzazione, è scritto anche nel WP136. Potranno tuttavia esserci alcune circostanze in cui le chiavi pubbliche e le impronte, per via delle modalità in cui in concreto vengono legittimamente impiegate o per il rischio di loro utilizzo da parte di terzi non autorizzati, potrebbero essere considerate alla stregua di dati personali, per la precisione pseudonimi[35].

5. *Coinbase e l'inserimento intenzionale di dati personali in blockchain*

Abbiamo appena visto che le soluzioni criptografiche che caratterizzano una blockchain non comportano necessariamente un tema di protezione di dati personali. È però possibile inserire deliberatamente in una blockchain dei dati personali in chiaro in modo che siano accessibili a chiunque da tutto il mondo senza possibilità di rimozione se non impiegando uno sforzo in termini di consenso ed energia molto consistente.

Nella blockchain dei bitcoin, per esempio, esiste un apposito spazio nell'intestazione dei blocchi chiamato *coinbase* a disposizione degli utenti per inserire messaggi di qualunque genere che, via via che nuovi blocchi "sedimentano", cioè si aggiungono nella sequenza della catena, diventano praticamente impossibili da rimuovere[36]. Altre blockchain, poi, potrebbero essere appositamente progettate in modo tale da non rispettare le disposizioni del GDPR ricorrendo, per esempio, all'impiego di chiavi pubbliche di firme digitali proprio allo scopo di identificare i soggetti interessati cui i dati in blockchain si riferiscono.

[35] Va sottolineato che il GDPR non definisce cos'è un dato pseudonimo, ma definisce la tecnica di pseudonomizzazione, ovvero il processo con cui si "nascondono" dei dati personali: «in modo tale che [questi] non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive» (art. 4, punto 5). Secondo il Regolamento, quindi, il dato pseudonimo nasce come dato personale e viene poi camuffato dietro una maschera alfanumerica. Ciò tuttavia non accade né con la chiave pubblica, né con l'impronta hash che nascono entrambe come dati semplici, non personali.

[36] Accenture ha creato una blockchain editabile utilizzando una funzione particolare chiamata *chamaleon hash* che consente di modificare i blocchi senza modificare anche le loro impronte hash ("Accenture to unveil blockchain editing technique", articolo apparso sul Financial Times 2016. Available at https://www.ft.com/content/f5cd6754-7e83-11e6-8e50-8ec15fb462f4).

In questi casi non è chiaro, secondo l'impostazione del Regolamento (e invero, come accennato all'inizio di questo lavoro, secondo una qualsiasi impostazione di legge), come potrebbe l'interessato pretendere il *diritto all'oblio* con la cancellazione dei suoi dati, né a chi dovrebbe rivolgere tale richiesta. Si presenterebbe infatti un insuperabile problema di *enforcement*, ovvero proprio il tipo di impedimento voluto dal movimento criptoanarchico che ha fatto germogliare e ha sviluppato la tecnologia blockchain.

6. *Titolari del trattamento in ambiente blockchain*

Se la chiave pubblica e l'impronta hash non sono dati personali, vien da sé che i nodi, fintanto che si limitano a svolgere le loro funzioni di *mining* e fintanto che il protocollo del network sia realizzato con un'architettura rispettosa del diritto alla protezione dei dati personali, non sono titolari del trattamento e non devono rispettare le disposizioni del GDPR[37]. Caricare su un server tutto o parte del database della blockchain al fine di validare i blocchi non costituisce di per sé un'operazione volta all'identificazione dei titolari delle chiavi pubbliche, né l'identificazione di questi è un effetto secondario ed immediato delle operazioni di *mining* o di *routing* del traffico. In tale prospettiva, nello spirito criptoanarchico che ha dato origine a questa rivoluzione tecnologica, chiunque può partecipare alla costruzione e rafforzamento di un network pubblico blockchain senza dover provvedere agli adempimenti previsti dal GDPR e senza dover adottare particolari misure di sicurezza.

Diverso è naturalmente il caso dei *wallet* e degli *exchange*, ovvero di tutti quegli ISP che raccolgono le opportunità di business offerte da una blockchain pubblica e in rete offrono servizi accessori agli utenti del network che vanno dalla gestione delle chiavi, allo scambio di criptovalute, e in futuro chissà cos'altro. Nel farlo trattano i dati personali dei propri clienti e quindi, come qualsiasi altro fornitore di servizi della società dell'informazione, debbono considerarsi a tutti gli effetti titolari del trattamento.

[37] Di diverso avviso è naturalmente M. Finck, op. cit., § IV(A), p. 16, il quale evidenzia le difficoltà di *enforcement* della disciplina del GDPR considerato il carattere distribuito della rete e l'enorme quantità di nodi e la loro multiterritorialità e continua mutevolezza.

7. *Conclusioni*

Nel prossimo futuro, l'ecosistema digitale si popolerà di reti peer-to-peer con protocollo blockchain[38]. Alcune saranno pubbliche, sviluppate con software open source, altre private, sviluppate con software proprietario, e altre ancora con architettura mista pubblico-privato. In tuti i casi i servizi veicolati saranno forniti adattandosi ad un nuovo modello di business che sfrutta l'orizzontalità del network decentralizzato e remunera i nodi con *token* o criptovalute di nuovo conio.

Non tutti i nodi saranno uguali sotto il profilo privacy. Alcuni tratteranno chiavi e impronte hash per fini identificativi più o meno diretti disponendo, o potendo ragionevolmente disporre, di liste di corrispondenza con l'identità dei soggetti interessati ad esse associati. Altri tratteranno le stesse chiavi e impronte al solo fine di consentire il funzionamento del network contando sulla remunerazione loro spettante per l'attività di *mining* e non avranno accesso ad alcuna lista di corrispondenza, né sarà previsto che lo abbiano. I dati da loro trattati, quindi, non saranno personali nel senso inteso dal Working Party e dalla CGUE, non essendo dati «relating to a natural person», difettando contenuto, scopo e risultato, e non essendo i soggetti interessati «indentifiable», mancando la ragionevole possibilità per loro di disporre di risorse e informazioni atte all'identificazione[39].

Di contro, un'interpretazione più ampia di dato personale che non tenga conto delle circostanze concrete di scopo del trattamento e di ragionevole possibilità di identificazione dei soggetti interessati, non solo sarebbe di ostacolo allo sviluppo della tecnica venendo contro all'evidente interesse dei cittadini e del mercato, ma si scontrerebbe con la pratica impossibilità di *enforcement* della legge risolvendosi di fatto in una sua disapplicazione generalizzata[40].

[38] Già esistono migliaia di reti blockchain che avranno forse un successo ancora più dirompente dei bitcoin. Un esempio per tutte è la rete Ethereum il cui numero di nodi (ethernodes.org/network/1) ha già superato quello dei bitcoin (bitnodes.earn.com).

[39] Come giustamente fa notare R. Bocchini, op. cit., p. 49, il nodo che si limita alle attività di validazione dei blocchi si comporta come un *mere conduit ex* art. 14 del d.lgs. n. 70/2003. Non solo quindi un nodo non assume gli obblighi di un titolare, ma neanche le responsabilità di *hosting* attivo.

[40] Su questo punto della "legge impossibile" è appropriato l'aneddoto di LL. Fuller, "The Morality of Law", «Yale University Press» 1969, pp. 36-37, richiamato da N. Purtova, op. cit., p. 2.

Il GDPR e la tecnologia blockchain non sono quindi ontologicamente incompatibili. Progettare un protocollo blockchain (pubblico o privato che sia) in modo tale che le soluzioni criptografiche impiegate non debbano considerarsi dati personali, e addirittura non debbano neanche considerarsi dati pseudonimi, è possibile, ed è anzi la regola[41], sicché la blockchain, anziché rappresentare un rischio per i diritti e le libertà fondamentali dell'individuo in termini di privacy, sarà lo strumento che metterà definitivamente nelle mani dei soggetti interessati la disponibilità esclusiva e il controllo dei loro dati[42].

[41] Non così M. Finck, op. cit., 27, il quale ritiene che i nodi debbano interrompere la validazione dei blocchi o attrezzarsi quantomeno adottato il DPIA *ex* art. 39 GDPR: «For the time being, the safest advice for blockchain developers is that transactional data should never be stored on a blockchain. Regarding public keys, the necessary risk-management solutions must be adopted and detailed Data Protection Impact Assessments must be carried out». Tale posizione non solo è impraticabile, ma va contro il funzionamento stesso dei network blockchain dove tutti i blocchi sono liberamente scaricabili e consultabili da chiunque.

[42] G. Zyskind, O. Nathan, A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", relazione del «Security and Privacy Workshops IEEE», 2015 (available at: https://enigma.co/ZNP15.pdf), in cui gli Autori illustrano l'architettura di un sistema decentralizzato di gestione dei dati personali.

I dati personali in ambiente blockchain tra anonimato e pseudonimato

Le chiavi pubbliche e le impronte hash costituiscono le due soluzioni criptografiche fondamentali con cui costruire una blockchain. Esse sono considerate dati pseudonimi pressoché in modo unanime, ossia dati personali mascherati dietro un codice, ma che possono nondimeno essere attribuiti ad un individuo specifico con l'ausilio di informazioni aggiuntive. Se ciò fosse vero, lo sviluppo della tecnologia blockchain sarebbe minacciato dal rispetto delle disposizioni del Regolamento Europeo 2016/679 sulla protezione dei dati personali (GDPR). Con il presene lavoro, intendo invece dimostrare che alla luce della definizione di dato personale, anche in forma di dato pseudonimo, contenuta già nella Direttiva 95/46/CE e oggi nel GDPR, non è possibile qualificare come tale né la chiave pubblica né l'impronta hash per come sono effettivamente impiegate nel protocollo blockchain originale dei bitcoin (e quindi, in generale, in protocolli *pemissionless* pubblici). Entrambe hanno infatti il solo scopo di risolvere un problema tecnico (il c.d. *double spending*), creando fiducia in un network con protocollo *peer-to-peer* e il loro eventuale utilizzo in sofisticate operazioni di *digital forensic* per rintracciare l'identità di titolari di indirizzi bitcoin, non le qualifica per ciò solo dati personali, né dati pseudonimi.

Personal data in blockchain environment between anonymity and pseudonymity

Public keys and hashes are the two fundamental cryptographic solutions commonly used to develop blockchain networks. They are considered almost unanimously pseudonymous data, that is personal data concealed behind an alphanumeric string that along with additional information can be nevertheless linked to a specific individual. If this were true, the development of blockchain technology would be hurdled by the necessity to comply with GDPR. In this paper, I held that the definition of personal data, even though in the form of pseudonymous data, set forth in Directive 95/46/EC and today in the GDPR (taking into account the CJEU interpretation and Article 29 Working Party opinion) does not apply neither to the public keys nor the hashes as they are used in a blockchain. They are not indeed used for concealing identities but to solve a technical problem (the so-called *double spending problem*) creating trust in a peer-to-peer network. Hence, although they could be (and sometimes they are) used to carry out advanced digital forensic searches to track down the identity of the private key holders, they are not actually designed to make or allow such searches and consequently they should be considered to be neither personal nor pseudonymous data.

Ciberspazio e Diritto vol. 19, n. 61 (3 - 2018), in questo numero:

Informatica giuridica

265 Autonomia e responsabilità nell'epoca delle *self-driving car*.
Teorie etiche a confronto,
Nicola Busto

279 Il cyberbullismo: le condotte tipiche e i soggetti coinvolti,
Samanta Stanco

315 Internet e l'epoca delle Costituzioni capillari:
il ruolo del costituzionalismo nella società digitale,
Andrea Venanzoni

Pubblica amministrazione digitale

319 La Pubblica Amministrazione nell'era delle ICT:
sportello digitale unico e intelligenza artificiale al servizio
della trasparenza e dei cittadini?,
Diana-Urania Galetta

Privacy, big data, profilazione e protezione dei dati

339 *Big data* e *people analytics:*
nuove sfide e opportunità per liberare valore
Ilenia Maria Alagna

359 La verifica preliminare dell'autorità di controllo su
disposizioni legislative o regolamentari,
Jean Louis a Beccara

369 La protezione dei dati personali nel cloud:
dati e rischi dal punto di vista dell'azienda,
Michela Cerullo, Edoardo Facchini,
Alessandra Lucchini, Paolo Pinto

385 La blockchain: una lettura giuridica per uno sguardo verso il futuro
Michele Chierici

421 Il consenso dell'interessato come condizione per l'offerta
di un servizio: la sentenza della Corte di Cassazione 17278/2018,
Lucrezia Falciai

431 Il binomio digitale "*influencer-storytelling*":
la nuova pubblicità e la tutela dei consumatori
Mariateresa Fiocca

457 I dati personali in ambiente blockchain
tra anonimato e pseudonimato
Francesco Rampone