Zambardino F, 'La blockchain e la protezione dei dati personali: una tecnologia privacy compliant by design?' (2022) 2 EJPLT, 1-..
DOI: …

EJPLT
ISSN 2704-8012

La *blockchain* e la protezione dei dati personali: una tecnologia *privacy compliant by design*?

Blockchain and the protection of personal data: a *privacy compliant by design* technology?

FABIO ZAMBARDINO
Dottore di Ricerca in Diritto Comparato e Processi di Integrazione presso la Università degli Studi della Campania "L. Vanvitelli"

Abstract

La tecnologia blockchain rappresenta un fenomeno rivoluzionario per diversi settori della vita dell'economia e non solo. Anzi, da un lato la necessità di adattare i tradizionali settori al cambiamento tecnologico, dall'altro le possibilità che tale tecnologia fornisce in termini di efficienza e velocizzazione, hanno portato la blockchain a essere presa sempre più in considerazione. La questione ancora in via di definizione, tuttavia, riguarda il trattamento dei dati, in un ecosistema trasparente e accessibile. L'obiettivo del presente scritto è, dunque, quello di analizzare l'impatto e le applicazioni di tale tecnologia in tutti i settori in qui essa è potenzialmente applicabile e, di conseguenza, le implicazioni in termini di privacy.

Keywords: Privacy, Blockchain, GDPR, trasparenza, decentralizzazione.

1. Introduzione.

Nell'odierno scenario globale, le nuove dinamiche della raccolta e del trattamento delle informazioni e dei dati personali, la maggiore invasività del controllo sugli individui, sia da parte di soggetti pubblici che privati, hanno comportato una sempre crescente richiesta di tutela[1].

Infatti, il centro gravitazionale del diritto alla *privacy* è sempre più individuato, più che nel diritto ad essere "lasciati soli" (il c.d. *right to be let alone*), nella possibilità di ogni soggetto di controllare l'uso delle informazioni che lo riguardano e nel considerare i problemi della *privacy* «nel quadro dell'attuale organizzazione del potere, di cui appunto l'infrastruttura informativa rappresenta ormai una della componenti fondamentali»[2].

Considerate le premesse, il presente scritto, dopo avere brevemente analizzato le circostanze che hanno portato alla nascita, sviluppo e conseguente tutela del concetto di *privacy*, si concentrerà sul rapporto che intercorre tra il diritto alla tutela dei dati personali e le nuove tecnologie, con particolare riferimento alla *blockchain*[3].

[1] Si veda, sul punto, G. RESTA, in G. ALPA e G. RESTA, *Le persone e la famiglia. Le persone fisiche e i diritti della personalità*, in *Trattato di diritto civile*, diretto da R. SACCO, Torino, 2019, 145-632, in cui viene privilegiato, in particolare, una interpretazione «orientata ai valori», considerata la linea maggiormente appropriata alla trattazione dei temi concernenti la persona e i diritti della personalità. In tale scenario, la globalizzazione dei mercati e l'evoluzione delle tecnologie costituiscono, per gli autori, complesse sfide al ruolo del diritto.

[2] S. RODOTÀ, *Tecnologia e diritti*, Bologna, 1995, 19.

[3] Parte della dottrina afferma come, alla stessa stregua i diritti di proprietà intellettuale, anche il diritto alla privacy è strettamente connesso alla tecnologia. L'evoluzione del concetto di privacy è proficuamente letta in chiave di diritto e tecnologia. G. PASCUZZI, U. IZZO, M. MACILOTTI (a cura di), *Comparative Issues in the Governance of Research Biobanks. Property, Privacy, Intellectual Property, and the Role of Technology*, Heidelberg-New York-Dordrecht-Londra, 2013. In argomento, G. PASCUZZI, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, Bologna, 2003. Secondo autorevole dottrina, sono i mutamenti delle tecnologie dell'informazione, della riproduzione e dell'ingegneria genetica a muovere il cammino che porterebbe dal diritto alla riservatezza (il diritto ad essere lasciato solo) al diritto di mantenere il controllo sulle proprie informazioni personali. S. RODOTÀ, Repertorio di fine secolo, Roma – Bari, 1999, 201. T. E. FROSINI, *Tecnologie e libertà costituzionali*, in G. COMANDÉ e G. PONZALLI (a cura di), *Scienza e diritto nel prisma del diritto comparato*, Milano, 2004, 189, il quale, ancora in tema di rapporto tra tecnologia e *privacy* afferma come le nuove scoperte tecnologiche abbiano rappresentato e continuino a rappresentare uno sviluppo delle libertà; «anzi, le libertà si sono potute notevolmente accrescere ed espandere verso nuove frontiere dell'agire umano proprio grazie al progresso tecnologico». T. E. FROSINI, *Il diritto costituzionale di accesso ad Internet*, in M. PIETRANGELO (a cura di), Il diritto di accesso ad Internet, Collana ITTIG-CNR, Serie "Studi e documenti", n. 9, Napoli, 2011, 24. Tra i primi a introdurre tali tematiche, sebbene in chiave più generale, S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari 1997.

2. Le origini e lo sviluppo del concetto di privacy.

Storicamente, i concetti giuridici di riservatezza e di *privacy* risalgono alla fine del XIX secolo. Infatti, è con l'articolo "*The Right To Privacy*"[4] di Warren e Brandeis del 1890 che la nozione di *privacy* ha iniziato ad assumere la connotazione giuridica descritta nel paragrafo introduttivo[5].

Di conseguenza, il vero riconoscimento del diritto alla *privacy* si è avuto dopo un lungo processo in cui un ruolo fondamentale ha avuto, inevitabilmente, la giurisprudenza[6].

Infatti, a tal proposito, il giudice William O. Douglas, nel caso *Griswold v. Connecticut*, ha affermato che un diritto generale alla privacy si trova nelle c.d. "*penumbras*" create dalle garanzie specifiche di diversi emendamenti della Carta dei Diritti[7].

Tuttavia, dopo la pubblicazione del "*The Right to Privacy*", l'elaborazione dottrinale statunitense in materia fu piuttosto scarsa, se non addirittura inesistente. Tale circostanza ha contribuito a rafforzare il ruolo dei giudici, i quali, con una serie di decisioni, «chiarirono alcuni principi dell'ordinamento giuridico americano e, cosa più importante, attraverso una interpretazione evolutiva degli emendamenti del Bill of Rights, riuscirono a rintracciare il fondamento giuridico del diritto alla privacy»[8].

Una spinta innovatrice si è avuta a partire dagli anni Sessanta del '900, quando i cambiamenti che sono derivati dal passaggio da uno Stato liberale tradizionale ad uno Stato pluralistico di diritto accrebbero la sensibilità verso le questioni inerenti alla tutela della sfera privata.

---

[4] S. WARREN e L. D. BRANDEIS, *The right of privacy*, in *Harv. L. Rev.*, 1890, 193.

[5] Per un approfondimento in tema di riservatezza, S. RODOTÀ, *Riservatezza*, in Enciclopedia Treccani, 2000. Si veda, inoltre, R. PARDOLESI, *Riservatezza: problemi e prospettive*, in M. SPINELLI (a cura di), *Responsabilità civile*, Bari, 1974, vol. II, 316 ss. L'autore, sul punto, già anni fa ha sostenuto come «l'informatica […] ha introdotto, sia nella raccolta che nel trattamento e nell'impiego di dati, un cambiamento quantitativo così radicale da volgersi in qualitativo». *Ivi*, 381. Ancora, l'autore sostiene, in riferimento alla nascita del diritto alla *privacy*, che alla stessa stregua dei diritti di proprietà intellettuale, si tratta di un prodotto recente della tradizione giuridica occidentale. *Ivi*, 391.

[6] In particolare, il riferimento va ai casi *Griswold v. Connecticut*, 381 U.S. 479 (1965), *NAACP v. Alabama*, 357 U.S. 449 (1958), *Katz v. U.S.* 347 (1967). L'opera dei giudici, infatti, non solo ha sollecitato fortemente il dibattito dottrinale in materia di *privacy* ma ha portato all'attenzione del legislatore le tematiche relative alla protezione della sfera privata, contribuendo così alla piena affermazione del diritto e alla sua tutela. Questo è quanto accaduto non solo negli Stati Uniti d'America ove il formante giurisprudenziale ha un posto privilegiato all'interno dell'ordinamento giuridico, ma anche all'interno di ordinamenti giuridici di *civil law* come quello italiano.

[7] J. B. STONEKING, *Penumbras and Privacy: A Study of the Use of Fictions in Constitutional Decision-Making*, in *West Virg. L. Rev.*, 1985, 859. Le garanzie esplicite del *Bill of Rights*, considerate collettivamente, sono state definite "*penumbras*" o "emanazioni" che «help [to] give them life and substance». In altre parole, i tribunali possono derivare dei diritti impliciti che sono necessari per dare piena attuazione a quelli espliciti. Si vedano, in proposito B. HENLY, *"Penumbra": The Roots of a Legal Metaphor*, in *Hastings Const. L. Q.*, 1987, 81, 83–84; G. H. REYNOLDS, *Penumbral Reasoning on the Right,* in *U. Pa. L. Rev.*, 1992, 1334–36; J. C. RIDEOUT, *Penumbral Thinking Revisited: Metaphor in Legal Argumentation*, in *J. ALWD*, 2010, 155–56.

[8] L. MIGLIETTI, *Profili storico-comparativi*, *cit.*, 2014. L'atteggiamento della giurisprudenza così come quello della società nei confronti dell'esigenza *privacy* fu però altalenante. Mentre una parte del tessuto sociale americano e una minoranza dei giudici della Corte Suprema «propugnavano un approccio difensivo della libertà e, nello specifico, della privacy; l'altra parte della società e la maggioranza dei giudici della Corte Suprema erano ostili verso un atteggiamento liberale e soprattutto verso il riconoscimento di un autonomo diritto alla privacy». Il riferimento è ai già citati casi *Griswold v. Connecticut*, *NAACP v. Alabama*, *Katz v. U.S. Ibid.* Questa antiteticità di vedute ha rappresentato non solo un ostacolo per lungo tempo all'elaborazione di una teoria in materia ma, soprattutto, non ha permesso di chiarire la natura del concetto, lasciandolo così alla mercé degli oscillanti orientamenti giurisprudenziali che si alternavano nel tempo.

Infatti, se fino a quel momento la giurisprudenza aveva assunto posizioni ancora non del tutto definite per quanto concerne il riconoscimento di un diritto alla *privacy* costituzionalmente garantito, a partire dagli anni Sessanta vennero emesse una serie di sentenze fondamentali con le quali la Corte Suprema riconobbe la *privacy* come meritevole di tutela in rapporto tanto alla vita pubblica quanto a quella privata dell'individuo[9].

Successivamente, nel 1970, venne emanata una legge, il *Privacy Act*, che ancora oggi rappresenta un importante testo normativo di riferimento in materia di privacy.

È opportuno sottolineare, che la mancanza «di una legislazione federale a vocazione generale che possa impartire un indirizzo comune ai vari Stati membri ha portato a qualificare il sistema di tutela della privacy statunitense come un sistema di natura settoriale. Le leggi degli Stati Uniti perseguono l'obiettivo di regolamentare il trattamento dei dati in ambiti specifici di attività economica, nella misura in cui vi possano essere rischi per il cittadino considerato nel suo status di consumatore»[10].

Ne consegue che negli USA, differentemente dall'Europa, la privacy non si configura come un diritto fondamentale dell'individuo, ma come un diritto del consumatore, da bilanciare con le esigenze delle imprese. Ed infatti è la FTC (*Federal Trade Commission*), l'agenzia deputata alla tutela dei consumatori negli States, competente a vigilare anche sull'aderenza dei comportamenti delle aziende a quanto esse dichiarano nelle proprie privacy policy e sul rispetto delle leggi sulla privacy[11].

Nell'ambito dell'Unione europea, contrariamente, lo sviluppo e la tutela del concetto di *privacy* ha vissuto fasi molto differenti. In tale contesto, infatti, il trattamento dei dati personali [12] è considerato, oggi, uno degli elementi maggiormente qualificanti del sistema giuridico europeo, il quale conferisce a tale diritto il medesimo valore riservato ai diritti fondamentali dell'uomo[13].

Inizialmente pensato in chiave di integrazione economica, la materia della *privacy* all'interno del sistema giuridico comunitario non era stato adeguatamente considerato e regolato attraverso specifiche disposizioni

---

[9] Negli stessi anni anche il dibattito dottrinale riprese vigore e tra le varie teorie elaborate fra tutte W. PROSSER, *Privacy*, in *Cal. L. Rev.*, vol. 48, 1960. La teoria di Prosser si basava sulla negazione del concetto unitario di *privacy* – concezione che invece avevano difeso Warren e Brandeis – sostenendo, al contrario, una concezione pluralistica. Qualche anno più tardi, nel 1964, Edward Blounstein pubblicò un saggio nel quale, rifiutando di accogliere l'elaborazioni teoriche di Prosser, propugnava il ritorno ad una visione unitaria della privacy, concepita come valore essenziale dell'uomo e come diritto meritevole di tutela in tutti gli ambiti normativi. E. J. BLOUNSTEIN, *Privacy as an aspect of human dignity: an answer to Dean Prosser*, in NYU *L. Rev.*, 1964, 974, sostiene «I contend that the gist of the wrong in the intrusion cases is not the intentional infliction of mental distress but rather ablow to human dignity, an assault on human personality. Eavesdropping and wiretapping, unwanted entry into another's home, may be the occasion and cause of distress and embarassement but that is not what makes these acts of intrusion wrongful. They are wrongful because they are demeaning of individuality, and they are such whether or not they cause emotional trauma». *Ibid.*

[10] L. MIGLIETTI, *Profili storico-comparativi*, *cit.*

[11] *Ibid.*

[12] Sulla nozione di trattamento dei dati, si veda L. LAMBO, *La disciplina sul trattamento dei dati personali: profili esegetici e comparatistici delle definizioni*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 75.

[13] Si vedano, in merito, L. BOLOGNINI, E. PELINO, C. BISTOLFI (a cura di), *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; R. CASO, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano*, in *Dir. Internet*, 2008, 466- 472.

normative, essendo quello della riservatezza un tema appartenente alla sfera dei diritti umani[14].

Tuttavia, si è provveduto alla tutela dei principi fondamentali della persona – e, di conseguenza, con essi anche la *privacy* – per merito della giurisprudenza della Corte di Giustizia dell'UE[15].

In siffatto scenario, nel momento stesso in cui il concetto di *privacy* ha assunto maggiore rilievo in seno alle istituzioni, considerato come un diritto a cui riservare una garanzia giuridica, si è diffusa l'espressione "*data protection*", ed è stato trasformato l'originario diritto alla riservatezza in un vero e proprio controllo specifico dei dati[16].

L'inizio della lunga e travagliata evoluzione normativa in materia di trattamento dei dati personali che ha avuto luogo in Europa è stato segnato dall'adozione della direttiva 95/46/CE del Parlamento Europeo e del Consiglio (cosiddetta "*Data Protection Directive*" o anche direttiva "madre")[17]. Con essa il legislatore europeo, oltre a prevedere un'accurata definizione di dati personali[18], ha recepito il nuovo profilo assunto dalla *privacy* al fine di tutelare i diritti e le libertà delle persone fisiche con specifico riferimento al trattamento dei dati e alla libera circolazione degli stessi, stabilendo altresì i principi relativi

---

[14] Per una attenta ricostruzione del dibattito sul tema, che ha animato la dottrina a partire dai primi decenni del Novecento, si veda S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, 39 ss. In Italia, per esempio, a ridosso della riforma del Codice civile, alcuni giuristi cominciarono a interessarsi al tema della "riservatezza", inquadrandolo nel contesto più generale dei diritti della personalità. A partire da quel momento in tema di diritto alla riservatezza si sviluppò un ampio dibattito dottrinale che vide coinvolti illustri giuristi e che trovò causa, anzitutto, nella mancanza di una norma esplicita e di portata generale che si ponesse a fondamento giuridico del sopraddetto diritto. In argomento, si vedano *ex multis* G. GIAMPICCOLO, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza nel quadro dei diritti della personalità*, in *Riv. Dir. Civ.*, 1963; A. DE CUPIS, *Teoria generale, diritto alla vita e all'integrità fisica, diritto sulle parti staccate dal corpo e sul cadavere, diritto alla libertà, diritto all'onore e alla riservatezza*, Milano, 1959; F. CARNELUTTI, *Il diritto alla vita privata*, in Rivista trimestrale di diritto pubblico, 1955; A. RAVÀ, *Istituzioni di diritto privato*, Padova, 1938.

[15] Per un approfondimento A. TERRASI, *Il rapporto tra diritto alla privacy e protezione dei dati personali tra Corte di giustizia dell'Unione europea e Corte europea dei diritti dell'uomo*, in M. DISTEFANO (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli, 2017, 127-149; R. CASO, *Misure tecnologiche di protezione: cinquanta (e più) sfumature di grigio della Corte di giustizia europea*, Trento Law and Technology Research Group. Research Papers, 2014. È interessante, a tal proposito, osservare la ricostruzione fatta da Gambaro, il quale, con riferimento alla libera circolazione dei dati personali, sottende la concezione di questi ultimi come beni giuridici oggetto di scambio. Per un approfondimento di tale pensiero si rimanda a A. GAMBARO, *I beni*, in *Tratt. dir. civ. e comm.*, già diretto da A. CICU e F. MESSINEO, continuato da L. MENGONI, Milano, 2012.

[16] In tema, si rimanda a G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012. L'autrice, in particolare, ben sintetizza l'evoluzione del termine. Infatti, comunque lo si pronunci, «è oramai polisenso e indica una molteplicità di beni giuridici e di interessi suscettibili di differente tutela». Il bene della riservatezza in senso stretto, ossia la tutela della vita privata, la segretezza, la privatezza dello spazio, la protezione delle informazioni. La pluralità e la diversità dei beni giuridici considerati «si riflettono anche nella scelta del legislatore europeo di disciplinare in maniera distinta la tutela della vita privata e la protezione dei dati personali, rispettivamente nell'art. 7 e nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea». G. FINOCCHIARO, *Il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, in Il *trattamento dei dati personali in ambito giudiziario*, Scuola Superiore della Magistratura, Roma, 2021, 21.

[17] F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 6.

[18] Art. 2, lettera a) della direttiva n. 95/46/CE definisce dati personali «qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale».

alla legittimazione degli stessi[19].

Nonostante le successive modifiche alla "direttiva madre" apportate con l'obiettivo di fronteggiare le nuove sfide derivanti dal crescente sviluppo della tecnologia delle comunicazioni che hanno richiesto, nel tempo, una maggiore tutela dei dati personali, l'impianto normativo europeo in tema di tutela della *privacy* è rimasto alquanto obsoleto, almeno fino all'entrata in vigore del *General Data Protection Regulation*[20].

3. L'introduzione delle Distributed Ledger Technologies.

L'utilizzo di *Distributed Ledger Technologies*, come la *blockchain*, si è esteso dal mercato delle criptovalute ad altri campi, incluso, per esempio, il settore della *privacy*[21].

In particolare, la necessità di decentralizzazione risiede nella crescente preoccupazione da parte degli utenti per la perdita di controllo in relazione ai propri dati personali registrati su Internet[22].

A questo proposito, la stessa struttura della tecnologia *blockchain* consentirebbe di preservare la riservatezza dei dati; tuttavia, tali architetture possono dimostrarsi talvolta vulnerabili all'analisi dei metadati. Di conseguenza, se non adeguatamente progettate, «decentralized infrastructures intended to promote individual privacy and autonomy might turn out to be much more vulnerable to governmental or corporate surveillance than their centralized counterparts»[23].

---

[19] L. BOLOGNINI e PELINO (a cura di), *Codice della disciplina privacy*, Milano, 2019. Sulle medesime tematiche, anche F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali: Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016. Gli autori, in particolare, propongono una lettura organica della vigente disciplina in materia di privacy e protezione dei dati personali, oggi estremamente frammentata e vasta in UE e in Italia, consentendo così un'immediata interpretazione della materia attraverso l'analisi combinata della normativa europea e di quella nazionale, nonché dei provvedimenti dell'Autorità Garante.

[20] F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH, *Il codice dei dati personali*, *cit.*, 9.

[21] Per una disamina dei diversi utilizzi della *blockchain*, A. BORRONI, *Blockchain: Uses and Potential Value*, in *Legal Perspective on Blockchain Theory, Outcomes, and Outlooks*, A. BORRONI (ed.), Pubblicazioni del Dipartimento di Scienze Politiche Jean Monnet dell'Università degli Studi della Campania Luigi Vanvitelli, ESI, 2019. Per un'analisi, invece, relativamente a possibili scenari regolamentari, si rinvia a A. BORRONI e M. SEGHESIO, *Bitcoin e Blockchain: Un'analisi comparatistica dalla nascita alla potenziale regolamentazione*, in *La relazione tra intermediari e clienti nel diritto dell'economia*, G. GIMIGLIANO (ed.), *IANUS Diritto e Finanza*, no. 19, 2019.

[22] Taluni autori, in proposito, fanno riferimento alla nascita di una vera e propria identità virtuale in quanto parlare di identità personale, nel contesto attuale, significa fare i conti anche con una nuova dimensione, ossia quella informatica, in cui l'identità personale risulta indispensabile per il compimento di una serie di azioni, per lo più di carattere patrimoniale – si pensi all'utilizzo delle carte di credito sul web, alle varie transazioni commerciali, fino ad arrivare ai social network. Su questo punto, S. RODOTÀ, *Quattro paradigmi per l'identità*, in *Vivere la democrazia*, Bari, 2018, 20 ss; G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, CONTR. IMPR., 2017, 725; G. RESTA, *Identità personale e identità digitale*, in *Dir. Infor.*, 2007. Per un primo approfondimento relativamente al rapporto tra *privacy* e *blockchain*, V. DEVI, V. SABARESHWARAN, R. SARAVANA KUMAR, M. SIVASANKAR, *Privacy-Preserving Healthcare Architecture Using Blockchain*, IJCSMC, vol. 9, 2020, 116-120; S. SAKHO *et al.*, *Privacy Protection Issues in Blockchain Technology*, IJCSIS, vol. 17, 2019, 124-131; R. DE LA CRUZ, *Privacy Laws in the Blockchain Environment*, in *Annals of Emerging Technologies in Computing*, vol. 3, 2019, 34-44; G. ALPA, *Tecnologie e diritto privato*, in *Rivista italiana per le scienze giuridiche*, 2017.

[23] P. DE FILIPPI, *The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies*, Paris, 2016, 1. Prima di approfondire la propria analisi, l'autore sottolinea come nonostante gli ovvi vantaggi che offrono per quanto riguarda la sovranità dei dati, le architetture decentralizzate presentano anche caratteristiche che, se non tenute in debita considerazione, potrebbero, in ultima analisi, compromettere la

In questa prospettiva, non va dimenticato che la natura pseudonima di molte reti che si basano sulla *blockchain* consente agli individui la possibilità di condurre le proprie transazioni su base *peer-to-peer*, senza la necessità di rivelare la propria identità alle controparti[24].

Allo stesso tempo, per converso, la trasparenza derivante dalle *distributed ledger technologies* è tale che chiunque ha la possibilità di accedere alla cronologia di tutte le transazioni memorizzate sulla *blockchain*, affidandosi così all'analisi dei dati in essa contenuti per ricavare informazioni potenzialmente sensibili[25].

In questo senso, tuttavia, laddove il sistema non sia progettato accuratamente, la trasparenza potrebbe finire per interferire con la *privacy* degli utenti[26].

Di conseguenza, a meno che non si utilizzino ulteriori mezzi tecnici per proteggere la riservatezza delle comunicazioni online, potrebbe risultare che le infrastrutture decentralizzate – progettate per promuovere la *privacy* e l'autonomia – finiscano per essere più vulnerabili alle agenzie governative o al controllo delle imprese rispetto alle loro controparti centralizzate[27].

Innanzitutto, il rapporto tra *privacy* e registri decentralizzati potrebbe, almeno all'apparenza, non risultare immediatamente calzante. In effetti, potrebbe sembrare più logico affermare che la *blockchain* sia meglio costruita al fine di preservare i dati e la *privacy* degli utenti[28].

A ogni modo, permane ancora un elevato livello di incertezza sulla potenziale predisposizione di soluzioni alternative – e decentralizzate – che siano in grado di affrontare adeguatamente il problema della riservatezza dei dati[29].

Indipendentemente da ciò, i sistemi decentralizzati, come la *blockchain*, hanno attirato crescente attenzione da parte della dottrina, che sta esaminando in maniera attenta come le DLTs potrebbero essere applicate in

---

privacy degli utenti. Infatti, «[w]hile they are capable of preserving the confidentiality of data, decentralized architectures cannot easily protect themselves against the analysis of metadata». *Ibid.*

[24] M. CROSBY, P. PATTANAYAK, S. VERMA, P. KALYANARAMAN, *Blockchain Technology Beyond Bitcoin*, Sutardja Center for Entrepreneurship & Technology, Berkeley University of California, 2015, 13-19. Mentre il bitcoin in sé è molto controverso, la tecnologia blockchain sottostante ha funzionato in modo impeccabile e ha dimostrato di poter trovare un'ampia gamma di applicazioni, sia nel mondo finanziario che in quello non finanziario. Tuttavia, tale tecnologia crea una situazione che, come avrebbe detto Rodotà, rappresenterebbe una realtà caratterizzata da un controllo permanente (ovvero di sempre maggiore ed indiscriminata identificazione ed identificabilità) dei singoli, come parti di un "gregge". Sul punto, si vedano S. RODOTÀ, *Il mondo nella rete: quali i diritti, quali i vincoli*, Roma-Bari, 2014; S. RODOTÀ, *Repertorio di fine secolo*, Roma-Bari, (1992-) 1999; S. RODOTÀ, *Tecnopolitica*, Bari, 1997.

[25] B. MARR, *A Very Brief History of Blockchain Technology Everyone Should Read*, Frobes, 2018. Disponibile al sito https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read. Consultato il 08 giugno 2022.

[26] D. BRADBURY, *The Problem with Bitcoin*, Computer Fraud and Security, 2013, 5-8.

[27] P. DE FILIPPI, *The Interplay*, *cit.*, 2.

[28] C. TRONCOSO, M. ISAAKIDIS, G. DANEZIS, H. HALPIN, *Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments*, De Gruyter Open, Proceedings on Privacy Enhancing Technologies, Losanna, 2017, 307-308. Sul punto, si afferma come sia possibile, in tal modo, una maggiore *privacy* dell'utente e, allo stesso tempo, un controllo autonomo dell'infrastruttura. In quanto tali, rappresentano una possibile soluzione tecnologica alle richieste delle leggi sulla protezione dei dati, vincolanti dal punto di vista giuridico ma spesso non applicate dal punto di vista tecnologico.

[29] Si consulti, inoltre, in tema di diritto alla riservatezza dei dati R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003; R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003.

relazione alla *privacy*[30].

Considerate quanto affermato finora, nelle pagine che seguono sarà analizzata la relazione che intercorre tra *privacy* e DLTs, il loro impatto in termini di vantaggi e svantaggi, e il rapporto tra trasparenza e *privacy* quando viene applicata la tecnologia crittografica.

4. I vantaggi in termini di privacy legati all'utilizzo della blockchain.

Quanto scritto in precedenza è principalmente riferito agli aspetti collegati alla sicurezza e alla privacy. In particolare, quando si fa riferimento a sistemi decentralizzati si fa riferimento a casi in cui non vi è alcuna entità che possa agire come una c.d. *Trusted Computing Base* (TCB) e che, in tale contesto, possa imporre degli standard di sicurezza o una politica di *privacy*[31].

Al fine di meglio comprendere le problematiche collegate alla protezione dei dati personali, è necessario considerare due aspetti rilevanti. *In primis* (i) l'identificazione del soggetto che si occupa della determinazione delle modalità in cui vengono trattati i dati personali e, in secondo luogo, (ii) l'individuazione del soggetto che si occupa di controllare il modo in cui i dati sono conservati e gestiti[32].

La decentralizzazione che caratterizza la *blockchain* non comporta solo più alti livelli di protezione per i dati personali degli utenti ma, al contempo, comporta un maggiore "potere" nelle mani degli stessi, in quanto gestiscono e hanno un completo controllo sulle informazioni che vengono scambiate tra di loro[33].

Infatti, la tecnologia *blockchain*, in questo senso, è stata definita da parte della dottrina come un «decentralized cloud computing system»[34].

In un siffatto scenario, il principale vantaggio che deriva dall'utilizzo di un sistema decentralizzato risiede nel fatto che viene data agli individui / utenti la possibilità di gestire e controllare in prima persona i propri dati.

Inoltre, i dati che vengono condivisi, generati e raccolti dagli stessi individui potrebbero essere resi disponibili e venduti per scopi comuni e, conseguentemente, utilizzabili anche da soggetti terzi, non diversamente da quanto accade con gli *open data* ma, ovviamente, con logiche e meccanismi differenti[35].

---

[30] C. TRONCOSO, M. ISAAKIDIS, G. DANEZIS, H. HALPIN, *Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments*, De Gruyter Open, Proceedings on Privacy Enhancing Technologies, Losanna, 2017, 308. Gli autori, in questo senso, forniscono anche la propria definizione di *distributed ledger technologies* asserendo che con tale concetto si fa riferimento a «[a] distributed system in which multiple authorities control different components and no single authority is fully trusted by all others». *Ibid.*

[31] J. RUSHBY, *A Trusted Computing Base for Embedded Systems*, Computer Science Laboratory, SRI INT'L, 1984, 294-311. Dal punto di vista definitorio, un *Trusted Computing Base* (TCB) si riferisce a tutti i componenti del computer che si combinano per fornire un ambiente sicuro nel sistema stesso per garantire la sicurezza delle sue informazioni.

[32] W. MAXWELL e J. SALMON, *A Guide to Blockchain and Data Protection*, Hogan Lovells, 2017, 10-11.

[33] *Ibid.*

[34] C. BRIDGE, *Blockchain's Next Frontier: Cloud Computing?*, in *Inv. Mark't Bus. Res.*, 2018. Concettualmente, in particolare, «[c]loud storage allows the user to store data and information online. This serves as a backup in case the data is lost and could be used to secure large amounts of data». *Ibid.*

[35] Si veda, sul punto, T. W. BELL, *Copyrights, Privacy, and the Blockchain,* in *Ohio North'n U. L. Rev.*, 2016, 461-466.

In aggiunta, per quel che concerne la struttura, la maggior parte delle architetture decentralizzate a disposizione degli utenti hanno lo scopo specifico di promuovere la *privacy* concentrandosi su almeno uno dei due paradigmi seguenti: riservatezza dei dati e la "sovranità" degli stessi[36].

Così analizzata, la decentralizzazione di cui è caratterizzata la *blockchain* ha il potenziale per ridurre effettivamente le asimmetrie informative che, generalmente, forniscono dei vantaggi agli operatori in sistemi centralizzati[37].

Proprio quest'ultimo aspetto merita di essere approfondito in maniera sostanziale; soprattutto se si considera che, al giorno d'oggi, ogni volta che un utente naviga in rete accetta innumerevoli *cookie* che monitorano le proprie attività *online*, le ricerche effettuate, le preferenze dei singoli individui[38].

La conseguenza di ciò risiede nel fatto che tutte le informazioni vengono profilate senza un adeguato e consapevole consenso[39].

5. Privacy contro trasparenza.

Tuttavia, va sottolineato come permangano, allo stato attuale, molteplici complessità per comprendere appieno il modo in cui *privacy* e trasparenza possano interagire tra essi.

Da un lato, in una società "trasparente", qualsiasi parte interessata può facilmente avere accesso alle informazioni. Ciò implica che la trasparenza sociale comporta la compromissione del diritto alla *privacy*. Di conseguenza, «è ragionevole associare alla crescente trasparenza delle informazioni un decrescente rispetto del diritto alla privacy»[40].

In siffatto scenario, quindi, la trasparenza che le DLTs sono in grado di offrire non è né assoluta né incondizionata. Infatti, le diverse tipologie di *blockchain* possono garantire diversi livelli di trasparenza[41].

In particolare, esistono due tipologie di *blockchain*, ossia vero le c.d. *permissionless* – che non necessitano di un'autorizzazione – e *permissioned* – che, al contrario, necessitano di autorizzazione. Soprattutto con riferimento a quest'ultima tipologia, le transazioni (o, comunque, gli scambi, la "scrittura"

---

[36] P. De Filippi, *The Interplay*, *cit.*, 4. Si veda, sul punto, anche S. Jin Kim, *An Impossible Trinity in Blockchain-based Transactions: Decentralization, Privacy, and Lower Transaction Costs*, Shanghaitech Sem Working Paper Series No. 2020-010, ShanghaiTech University, 2020.

[37] *Ibid.* Sul medesimo punto, si veda per un approfondimento anche A. T. Themelis, *Information and Intermediation, Abuse of Dominance and Internet 'Neutrality': 'Updating'Competition Policy under the Digital Single Market and the Google Investigations (?)*, *EU. J. L. & Tech*, Vol. 4, no 3, 2013.

[38] Per quel che concerne la fruizione di servizi in rete, G. Resta e V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, *Riv. Trim. Dir. Proc. Civ.*, fasc. 2, 2018; S. Rodotà, *Il mondo della rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014.

[39] S. Goldfeder, H. Kalodner, D. Reisman, A. Narayanan, *When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies*, Sciendo, Proceeding on Privacy Enhancing Technologies, Vol. 2018, issue 4, 2018, 189-191. Per una disamina della fattispecie della revoca del consenso, si veda, G. Resta, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, *Riv. Crit. Dir. Priv.*, 2000.

[40] Sia consentito riferimento a F. Zambardino, *La blockchain nel mercato del lavoro italiano con particolare enfasi sulla questione privacy e il rapporto con il General Data Protection Regulation*, in TSL, 2022, 23-38. Si veda, inoltre, G. R. Mayes, *Privacy and Transparency*, Sacramento State University, Department of Philosophy, 2018, 125-129.

[41] M. Seghesio, *Blockchain and Privacy,* in *Legal Perspective on Blockchain Theory, Outcomes, and Outlooks,* A. Borroni (ed.), Pubblicazioni del Dipartimento di Scienze Politiche Jean Monnet dell'Università degli Studi della Campania Luigi Vanvitelli, ESI, 2019, 138.

delle informazioni) avvengono all'interno di un ecosistema chiuso, in cui tutti i dati registrati rimangono, in un certo modo, riservate e le identità dei partecipanti sono note[42].

Da un punto di vista pratico, i problemi di *privacy* derivanti dal livello di trasparenza della *blockchain* possono essere mitigati «dalla crittografia della comunicazione "end-to-end", la quale richiede chiavi private e pubbliche, anziché utilizzare una chiave unica per la crittografia e la decrittografia»[43].

Il principio afferma che, laddove possibile, le operazioni del protocollo di comunicazione devono essere definite per essere effettuate ai punti finali di un sistema di comunicazione, o il più vicino possibile alla risorsa da controllare[44].

In particolare, crescono le aspettative sociali per quel che concerne la trasparenza e la supervisione degli algoritmi e nel rendere i sistemi decisionali automatizzati responsabili, più trasparenti e governabili, eventualmente dotandoli di nuovi strumenti tecnologici in grado di verificare che le decisioni automatizzate siano conformi a standard chiave di equità giuridica. Garantire la responsabilità attraverso valutazioni d'impatto degli algoritmi (AIA), audit e certificazioni dovrebbe essere parte integrante di tutte le iniziative politiche e legali in questo campo, considerando che la *blockchain* allo stato attuale non è stata ancora compiutamente implementata[45].

6. Prime riflessioni. Quali implicazioni in termini di sovranità statale.

Uno dei problemi principali legati all'utilizzo di una simile tecnologia – così come, in generale, anche per Internet – è rappresentato dalla crescente tensione «fra il bisogno di una rete aperta e autenticamente globale e l'affermazione di diritti di sovranità sul proprio territorio e sui propri cittadini richiede, per risolverla, più della semplice buona volontà»[46].

Il primo punto da considerare è di natura ideologica. Per lungo tempo, l'idea dominante è stata che la *blockchain*, alla stessa stregua dell'IoT, in quanto globale, sia essenzialmente aterritoriale e, di conseguenza, può "esistere" grazie a regole auto-determinate.

---

[42] PARLAMENTO EUROPEO, *What if blockchain offered a way to reconcile privacy with transparency?*, Unione Europea, 2018. Disponibile al sito europa.eu/RegData/etudes. Consultato il 08 giugno 2022.

[43] F. ZAMBARDINO, *La blockchain nel mercato del lavoro italiano*, *cit.*, 25-26. Per un approfondimento del concetto di comunicazione *end-to-end*, si veda L. ZHANG, *End to end architecture and mechanisms for mobile and wireless communications in the Internet*, Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS, Institut National Polytechnique de Toulouse, Université de Toulouse, 2009, 7.

[44] Con riferimento ai rischi, si veda B. GARDELLA TEDESCHI E S. THOBANI, *Innovazione, diritto e tecnologia: temi per il presente e il futuro. Introduzione*, in *Rivista di Diritto dei Media*, 2020, secondo cui i rischi derivanti dall'automatismo, in particolare, sono acuiti dall'invasività delle nuove tecnologie, che consentono un elevato grado di intrusione nella vita privata delle persone. L. ZHANG, *End to end architecture*, *cit.*, 7-8. Il principale vantaggio di sistemi di comunicazione "end-to-end" è rappresentato dal fatto che consente di integrare «efficient and intelligent mechanisms at the end systems and doesn't require the modifications to the intermediate system, which make the de- ployment easier and much more flexible». *Ibid.*

[45] L. ZHANG, *End to end architecture*, *cit.*, 3. Si vedano, per un approfondimento sul tema, D. REISMAN, J. SCHULTZ, K. CRAWFORD, M. WHITTAKER, *Algorithmic Impact Assessment: A Practical Framework for Public Agency Accountability,* AINOW Institute, 2018. Disponibile al sito https://ainowin- stitute.org/aiareport2018.pdf. Consultato il 08 giugno 2022.

[46] V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. RESTA e V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Consumatori e Mercato, Roma, 2016, 14.

Volendo osservare la questione da una prospettiva della sovranità degli Stati, la *blockchain* può essere considerata alla stessa stregua di un protocollo utilizzato al fine di per trasferire pacchetti di dati, utilizzando reti pubbliche (*i.e.* aperte al pubblico). È chiaro che un protocollo di questo tipo ha consistenza giuridica nel settore della proprietà intellettuale e dal punto di vista regolamentare, «ma essendo interamente non materiale esso non può formare oggetto di sovranità più di uno standard di telecomunicazione o di un sistema di misurazione metrico decimale»[47].

In aggiunta, il fatto che le informazioni che vengono trasmesse in un ecosistema di questo tipo siano intangibili e vengano inviati sulla base di una entità non materiale (come il protocollo Internet) non significa necessariamente che la rete sia immateriale. Anzi, piuttosto essa è composta in larga misura da elementi fisici, collocati quasi interamente sul territorio sovrano dello Stato[48].

Tuttavia, è innegabile come l'epoca contemporanea abbia presentato dei casi sempre più frequenti di regimi che operano senza essere necessariamente contenuti all'interno di un sistema incentrato sugli ordinamenti statali, «pur mantenendo per lo più qualche rapporto con esso, oppure ponendosi con esso, in vario modo, addirittura in contrasto»[49].

Tuttavia, da lì ad affermare che in questi casi si possa considerare l'esistenza di un unico ordinamento giuridico "globale" o "universale" sarebbe quantomeno improprio, soprattutto in considerazione del fatto che i diversi sistemi di regole statali e transnazionali interagiscono al fine di dare vita a una regolamentazione anche in relazione alle attività condotte nelle reti digitali[50].

7. Quale rapporto con il General Data Protection Regulation (GDPR).

Nelle pagine precedenti è stato osservato come, per definizione, la *blockchain* è un archivio distribuito; come naturale conseguenza, anche il controllo sui dati personali non può che essere decentralizzato, demandato a

[47] *Ibid.* ancora, l'autore, con riferimento specifico a Internet – ma per analogia il medesimo discorso è applicabile anche alla *blockchain* – afferma come non possa esservi sovranità sul protocollo Internet più di quanta ce ne possa essere sui protocolli utilizzati per i servizi Skype o WhatsApp.

[48] *Ibid.* L'autore ben esemplifica come l'unico caso di comunicazione extra-territoriale non-materiale è «quella di un messaggio proveniente da un satellite ricevibile direttamente dall'utente (ad es. con un telefono mobile satellitare) senza bisogno di una infrastruttura terrestre che lo distribuisca». Sul punto, V. M. MEJIA-KAISER, *Space Law and Unauthorised Cyber Activities*, in K. ZIOLKOWSI (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 349.

[49] C. PONCIBÒ, *Il Diritto Comparato e la Blockchain*, Memorie del Dipartimento di Giurisprudenza dell'Università di Torino, Napoli-Torino, 2020, 226. Del medesimo autore, anche C. PONCIBÒ, *Blockchain and Comparative Law*, in B. CAPPIELLO e G. CARULLO (eds.), *Blockchain, Law and Governance*, 2020,137-156.

[50] *Ibid.* Del medesimo avviso, G. PASCUZZI, *Il diritto dell'era digitale*, V ed., Bologna, 2020; O. POLLICINO, L. LIGUORI, G. BUSIA (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali*, Roma, 2016. Sul punto, uno spunto di riflessione è fornito da G. TEUBNER, *Ordinamenti frammentati e costituzioni sociali*, in *Rivista giuridica degli studenti dell'Università di Macerata*, 2010, 45-57, il quale afferma come sia opportuna, se non anche auspicabile, «una dilatazione semantica del nostro concetto di diritto, in modo tale che esso possa includere anche le norme operanti a prescindere dalle fonti giuridiche dello stato o del diritto internazionale».

tutti i partecipanti della *blockchain*. Tuttavia, una sorta di controllo centralizzato è prevista nel testo del GDPR[51].

Infatti, al fine di perseguire il duplice obiettivo della protezione dei dati e, al contempo, della libera circolazione degli stessi nel mercato interno, l'Unione europea ha optato per un ambizioso quadro di protezione dei dati, il *General Data Protection Regulation* (di seguito, GDPR), sostituendo la Direttiva 95/46/CE[52].

Il GDPR, specificamente, si prefigge come obiettivo cardine quello di garantire «un elevato livello di protezione dei dati personali, ponendo un freno alla frammentazione normativa in materia prodotta dalla diversa attuazione, nei vari Stati membri, della precedente Direttiva»[53].

La strada attraverso la quale il Regolamento si propone di giungere a tale obiettivo si muove lungo due direttrici fondamentali: da una parte, attraverso la "responsabilizzazione" maggiore dei soggetti attivi del trattamento; dall'altra, fornendo agli interessati strumenti specifici tesi ad innalzare il livello di consapevolezza sull'uso dei propri dati[54].

A partire dal 25 maggio 2018, tale Regolamento è divenuto direttamente applicabile in tutti gli Stati membri dell'Unione europea[55].

In particolare, il GDPR, come indicato dalla stessa Commissione Europea, ha lo scopo, tra gli altri, di garantire la certezza e l'armonizzazione del diritto in materia di protezione dei dati personali nonché una maggiore semplificazione delle norme sul medesimo punto.

In tale prospettiva, il Regolamento si pone come una risposta necessaria e propositiva alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di protezione dei dati personalità sempre più sentite dai cittadini dell'UE[56].

---

[51] M. FINK, *Blockchain and Data Protection in the European Union*, in *Eur. Data Prot. L. Rev.*, 2017, 9. Per un approfondimento, si veda anche G. ALPA, *La "proprietà" dei dati personali,* in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, Milano, 2019.

[52] *Ibid.* In particolare, per 'dato personale', nello specifico contesto del GDPR si intende qualunque tipo di informazione che possa ricondurre a uno specifico individuo. Analizzando questa definizione è possibile evincere fin da subito che la questione è piuttosto complessa. Infatti, la *blockchain*, sempre in quanto sistema distribuito, rappresenta uno strumento potenzialmente incontrollabile e, quindi, può non garantire appieno la tutela dei dati personali così come stabilito dal GDPR. R. TEPERDJIAN, *The Puzzle of Squaring Blockchain with the General Data Protection Regulation*, in *Jurimetrics J.*, 2020, 293-294.

[53] A. M. GAMBINO e C. BOMPREZZI, *Blockchain e protezione dei dati personali*, in *Dir. Infor.*, 2019, 620. Ancora in tema di rapporto tra GDPR e tutela dei dati personali G. ALPA, *La "proprietà" dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, N. ZORZI GALGANO (a cura di), Milano, 2019, 17 ss.

[54] *Ibid.* Entrambe le linee d'azione, nello specifico, se complessivamente considerate, producono «come effetto quello di un innalzamento del livello di controllo sui dati, come già auspicato dal Garante europeo della protezione dei dati». *Ibid.* Sul punto, anche A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (Artt. 32-39)*, in G. FINOCCHIARO, (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, 2017, 287 ss.

[55] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. Disponibile al sito https://eur-lex.europa.eu/legal-content/IT/TXT. Consultato il 08 giugno 2022.

[56] *Ibid.* Si vedano, sul punto, anche S. SATER, *Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows*, Tulane University, 2017, 4-7; C. SALMENSUU, *The General Data Protection Regulation and Blockchains*, University of Helsinki, Tieto, 2018.

Il cuore del GDPR risiede nella protezione dei dati degli utenti. Più specificamente, il regolamento riconosce «(i) il diritto alla portabilità dei dati[57], (ii) il diritto all'oblio[58] (il quale, prima dell'entrata in vigore del regolamento, era riconosciuto solo dalla giurisprudenza), (iii) il diritto di essere informato in un modo trasparente, corretto e dinamico sul trattamento dei dati, (iv) il diritto di essere informati in maniera tempestiva su qualsiasi violazione dei dati personali (*data breach*)»[59].

Il fatto che le trasmissioni siano intangibili non significa che lo Stato non possa, di fatto o di diritto, impedire la circolazione di taluni contenuti, l'accesso a siti stranieri, o l'accesso dall'esterno a siti interni, e in generale non possa legittimamente. Tutti questi interventi evidenziano come gli Stati – o nel caso dell'UE, entità sopra-nazionali – esercitano i loro poteri sulle reti di telecomunicazioni, da aspetti di poco rilievo fino a interventi assai più complessi e profondi. In tale ottica, stabilire come i dati personali raccolti «attraverso le reti di telecomunicazioni debbano e/o possono essere elaborati e a quali condizioni essi possano essere trasferiti in altri paesi costituisce semplicemente l'espressione dell'esercizio di poteri sovrani da parte e secondo uno stato di diritto»[60].

Tenendo presenti le importanti distinzioni tra le varie forme di DLTs e la necessità di un'analisi caso per caso che ne deriva, di seguito il tentativo di fornire una panoramica generale dell'applicazione del GDPR alla *blockchain*, «con focus sulla questione se i dati relativi a una persona fisica archiviati in un registro decentralizzato possano essere qualificati o meno come dati personali ai sensi del diritto europeo»[61].

---

[57] Per un'analisi sul diritto alla portabilità dei dati, si rinvia a L. BIANCHI, *Il diritto alla portabilità dei dati*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Reg. UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003*, Milano, 2019.

[58] Art. 17 del GDPR. Tale disposizione prevede che il titolare dei dati ottenga dal controllore «the erasure of personal data concerning him or her without undue delay». I titolari del trattamento sono obbligati a cancellare i dati personali soggetti a una serie di condizioni, come «(i) that personal data is no longer necessary for the purposes it was collected or otherwise processed; (ii) that the data subject withdraws consent on which the processing is based or where there is no other ground for processing; (iii) that the data subject objects to the processing and that there are no overriding legitimate grounds for processing; that (iv) data has been unlawfully processed; (v) that personal data has to be erased for compliance with national or supranational law to which the controller is subject; or that (vi) personal data has been collected in relation to the offer of an information society service to a child under 16 years of age». M. FINK, *Blockchain and Data Protection*, *cit.*, 23. Per una disamina del concetto giuridico di oblio, si vedano A. PALMIERI e R. PARDOLESI, *Polarità estreme: oblio e archivi digitali*, FORO IT., 2020, parte I, 1570 (nota a Cass., sez. I, 27 marzo 2020, n. 7559); R. PARDOLESI, *Oblio e anonimato storiografico: «usque tandem...»?*, in *Foro It.*, 2019, parte I, 3082 (nota Cass., sez. un., 22 luglio 2019, n. 19681); S. MARTINELLI, *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in Internet e le problematiche poste dalla de-indicizzazione*, DIR. INFOR., 2017; R. PARDOLESI, *Diritto all'oblio, cronaca in libertà vigilata e memoria storica a rischio di soppressione*, in *Foro It.*, 2016, parte I, 2734 (nota Cass., sez. I, 24 giugno 2016, n. 13161).

[59] F. ZAMBARDINO, *La blockchain nel mercato del lavoro italiano*, *cit.*, 27. Si veda anche Regolamento (UE) 2016/679, *cit.* Si vedano, sul punto, A. LONGO e R. NATALE, *GDPR, tutto ciò che c'è da sapere per essere in regola*, Agenda Digitale, 2018. Disponibile al sito https://www.agendadigitale.eu. Consultato il 08 giugno 2022. N. BOLDRINI, *Blockchain e GDPR: le sfide (e le opportunità) per la protezione dei dati*, Blockchain4Innovation, 2018. Disponibile al sito https://www.blockchain4innovation.it/sicurezza/blockchain-gdpr/. Consultato il 08 giugno 2022.

[60] V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems*, *cit.*, 10. L'autore afferma come, «il problema […] non è quello di stabilire quale diritto privato debba applicarsi al rapporto giuridico e chi sia il giudice competente. Quel che è in gioco in questi casi, invece, è la regolazione pubblica delle reti, che non può essere risolto attraverso le regole applicabili ai soggetti privati». *Ibid.*

[61] F. ZAMBARDINO, *La blockchain nel mercato del lavoro italiano*, *cit.*, 27-28. Sul medesimo punto, anche M. FINK, *Blockchain and Data Protection*, *cit.*, 9.

Pertanto, proprio in tale ottica, l'analisi dell'interazione tra la *blockchain* e il GDPR trova giustificazione. In particolare, se da un lato sarebbe utile valutare se tale tecnologia possa effettivamente essere utilizzata per facilitare la tutela della *privacy*, dall'altro lato è pur vero che la tecnologia *blockchain* non viola nessuna delle disposizioni del regolamento[62].

In siffatto scenario, l'art. 25 del GDPR, relativo alla *data protection by design* richiede al titolare del trattamento di mettere in atto «misure tecniche e organizzative adeguate […] volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente Regolamento e tutelare i diritti degli interessati»[63].

Pertanto, si può dedurre che si prediligono soluzioni volte a favorire (i) la minimizzazione dei dati contenuti, (ii) la trasparenza, in relazione all'utilizzo dei dati raccolti, nonché (iii) il permesso all'interessato di esercitare un adeguato controllo sui propri dati[64].

Da quanto fin qui emerso, pare che le caratteristiche della *blockchain* possano soddisfare i desiderata del GDPR circa la necessità di una protezione dei dati sin dalla progettazione. Pertanto, è possibile affermare che, a questo proposito, la *blockchain* può essere considerata ideale per la protezione dei dati personali in quanto ha intrinsecamente il compito di «data protection by design»[65].

Per quel che concerne la *compliance* tra Regolamento e *blockchain* è necessario analizzare sia quelli che sono i punti di conflitto che di convergenza; in questo senso, infatti, sebbene il GDPR e la *blockchain* condividano diversi

---

[62] *Ibid*. Secondo le previsioni annunciate all'ultimo *World Economic Forum*, entro il 2025 ben il 10% del PIL mondiale sarà prodotto da attività e servizi che saranno prodotti e distribuiti attraverso le tecnologie blockchain. Uno scenario, questo, che dovrà fare i conti con le normative, prima fra tutte il GDPR, appunto.

[63] Le caratteristiche che la tecnologia adottata dovrebbe avere a tal fine sono meglio specificate al considerando n. 78 del Regolamento, 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». A. M. Gambino e C. Bomprezzi, *Blockchain e protezione dei dati personali*, *cit.*, 624-625.

[64] . Zambardino, *La blockchain nel mercato del lavoro italiano*, *cit.*, 29. Sottolineano tale elemento positivo, tra gli altri, M. Berberich e M. Steiner, *Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?*, in *Eur. Data Prot. L. Rev.*, 2016, 425 ss.

[65] Su questo punto, si veda C. Lima, *Blockchain-GDPR Privacy by Design. How Decentralized Blockchain Internet will Comply with GDPR Data Privacy*, Blockchain Engineering Council, IEEE Blockchain Standards, 2018, 2-5. Disponibile al sito https://blockchain.ieee.org. Consultato il 08 giugno 2022. Secondo l'autore, considerando che la tecnologia *blockchain* non consente agli utenti di ripercorrere i propri passi ed eliminare o modificare i dati in essa inseriti, è più che mai indispensabile applicare il principio della *privacy by design*.
Quanto appena affermato, in particolare, trova conferma sotto 3 aspetti fondamentali: (i) le *blockchain* sono decentralizzate e distribuite, aspetto che rende molto più difficile che un attacco di *cybercrime* possa andare a buon fine; (ii) le *blockchain* sono pubbliche e trasparenti per l'utente, il che significa che le informazioni sulle transazioni sono pubbliche ma l'identità e i dati personali sono "mascherati" da una chiave pubblica il cui contenuto è noto solo al diretto interessato; (iii) le *blockchain* fanno un ampio ricorso alla crittografia e sfruttano il meccanismo degli incentivi garantendo, almeno a livello teorico, un metodo sicuro per archiviare e gestire le informazioni (compresi, ovviamente, anche i dati personali). Si vedano, per un approfondimento sul punto, B. S. Jiménez-Gómez, *Risks of Blockchain for Data Protection: A European Approach*, in *Santa Clara High Tech. L. J.*, 2020, 281-343; A. Mirchandani, *The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR*, in *Fordham Intell. Prop. Media & Ent. L. J.*, 2019, 1201-1241.

aspetti, va sottolineato che il Regolamento europeo non è stato redatto *ad hoc* per essere compatibile con un sistema decentralizzato[66].

Pertanto, l'estensione efficace ed efficiente delle disposizioni del GDPR alla tecnologia *blockchain* è subordinata alla previa interpretazione di giudici e regolatori[67].

In particolare, se si considera l'applicazione del GDPR su *blockchain* pubbliche e, quindi, *permissionless*. Nei confronti di tale tipologia di *blockchain*, infatti, l'applicazione del Regolamento può rivelarsi di non agevole realizzazione, dato che la semplice idea di un diritto alla cancellazione si pone in netto contrasto tutto ciò che rappresenta la *blockchain*[68].

In questo contesto, infatti, dopo che una chiave pubblica e le transazioni associate sono state identificate, non c'è modo di "cancellare" le informazioni, che fanno parte della *blockchain* e, quindi, di dominio pubblico.

Sono state anche sollevate questioni su come sarà possibile per le *blockchain* aderire al principio di minimizzazione dei dati, dato che i dati vengono continuamente aggiunti alla catena senza possibilità di cancellazione o modifica e le *blockchain* sono in continua crescita[69].

Sul punto, in particolare, uno degli elementi di contrasto maggiormente evidenti con il GDPR risiede nel fatto che la *blockchain* si basa su un sistema di registro distribuito, decentralizzato e immutabile[70].

Questa funzionalità significa che (i) i dati inseriti nella *blockchain* sono pubblici e accessibili da chiunque partecipi alla rete, (ii) non vi è alcuna

---

[66] K. SWAMINATHAN, *Blockchain Versus GDPR and Who Should Adjust Most*, Finextra, 2018. Disponibile al sito https://www.finextra.com/blogposting/16102/blockchain- versus-gdpr-and-who-should-adjust-most. Consultato il 08 giugno 2022. La tematica in questione è, sicuramente, pertinente se si considera che la tecnologia *blockchain*, per sua propria natura, non consentirebbe la cancellazione dei dati. Infatti, «[w]ithout entering the technical specifications, as soon as a data is entered and shared in the network it cannot be deleted without compromising the reliability, security and validity of the Blockchain system itself. The entry of the data is, therefore, an irreversible process». *Ibid.*

[67] M. FINCK, *Blockchains and Data Protection in the European Union*, EDPL, 2018, 21-26.

[68] M. KRITIKOS, *What if blockchain offered a way to reconcile privacy with transparency?,* European Parliament Research Service, Scientific Foresight Unit (STOA), 2018, 2. Disponibile al sito https://www.europarl.europa.eu/RegData/etudes. Consultato il 08 giugno 2022. In merio al diritto alla cancellazione, si approfondisca con A. BERTI SUMAN, *Il diritto alla cancellazione*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Reg. UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003*, Milano, 2019.

[69] *Ibid.* in particolare, «[t]he spirit of data minimization is profoundly at odds with data storage on a DLT». M. FINK, *Blockchain and Data Protection*, *cit.*, 20. Inoltre, il GDPR prevede che i dati personali siano «collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes». Art. 5, comma 1, let. b), del GDPR. Inoltre, un altro aspetto importante evidenziato da tale articolo è che i dati pesrsonali devono essere «lawfully, fairly and transparently processed in regards to the data subject». Il principio di correttezza, in particolare, va ritrovato in tutto il Regolamento, a partire dai diritti dell'interessato e passando per elementi importanti come l'operatore e l'incaricato del trattamento, i trasferimenti di dati verso Stati terzi o organizzazioni internazionali, il ruolo dell'Autorità nazionale, in particolare per quanto riguarda l'applicazione di sanzioni. D. M. SANDRU, *The fairness principle in personal data processing*, in *Law Review*, vol. 10, 2019, 61. Del medesimo autore, si vedano anche, D. M. SANDRU, *Elements regarding the regulation of the consent in the processing of personal data, according to article 6 of Regulation 2016/679*, in *Revista romînă de dreptul afacerilor*, no. 1, 2018; D. M. SANDRU, *The Impossible Coexistence between Data Protection and Virtual Communities? What's next?*, in *Pandectele romîne*, no. 1, 2018, 17-25.

[70] M. SEGHESIO, *Blockchain and Privacy*, *cit.*, 144. In questo senso, infatti, il GDPR è stato progettato per essere uno "strumento" indipendente. In particolare, i requisiti principali per la cancellazione e la modifica dei dati sembrano essere in conflitto con il modo in cui funziona la tecnologia *blockchain*. In effetti, «the blockchain is intended to be a permanent and tamper-proof record that lies outside the control of any government authority». *Ibid.*

possibilità di rimuovere i dati che siano stati effettivamente aggiunti[71] e (iii) non esistono limitazioni di alcuna sorta per quanto riguarda i dati che possono essere memorizzati sulla *blockchain*[72].

Pertanto, prima di proseguire oltre nell'analisi, sarebbe necessario capire come la protezione dei dati personali, in generale, possa essere riconciliata con un sistema in cui vengono immagazzinate enormi quantità di dati e, in secondo luogo, come le regole relative al tempo di conservazione dei dati all'interno di un siffatto sistema possano essere valide[73].

Per quel che concerne gli elementi di contrasto, innanzitutto, non va sottovalutato il fatto che, alla luce della considerazione che le informazioni non possano essere modificate o cancellate, qualora la *blockchain* dovesse essere fattivamente utilizzata come una sorta di *database* che tratta i dati personali, in base alla propria struttura, violerebbe il GDPR. In aggiunta, poiché la tecnologia *blockchain* è un sistema decentralizzato, sarebbe impossibile, di diritto, identificare un unico responsabile della protezione dei dati, come espressamente richiesto dal GDPR[74].

Queste, in particolare, così come altre caratteristiche della *blockchain* vanno a scontrarsi con quelli che sono gli elementi che caratterizzano le architetture di gestione centralizzata dei dati, che rappresentano ancora, allo stato attuale, l'unica tipologia di architettura che il regolatore aveva in mente quando è stato redatto il GDPR[75].

Dopotutto, l'intento primario dei legislatori europei, sotto il profilo regolamentare, con il GDPR era quello di fornire un paracadute giuridico per le attività degli attori privati, in particolare le nuove società che operano *online*, i cui modelli di business si basano sulla tecnologia *data-driven*[76].

---

[71] Si veda, per un approfondimento sul punto, M. Conoscenti, A. Vetrò, J. C. De Martin, *Blockchain for the Internet of Things: A Systematic Literature Review*, Nexa Center for Internet & Society DAUIN-Politecnico di Torino, 2016.

[72] K. Swaminathan, *Blockchain Versus GDPR*, *cit.* A tal proposito, va evidenziato che tra i diritti dell'individuo, secondo il regolamento GDPR, ci sono quelli di cancellazione, rettifica e modifica dei dati personali. In un sistema centralizzato l'interessato può esercitare tali diritti rivolgendosi al titolare del trattamento. Ovviamente, tutto ciò è diverso nel caso dei sistemi decentralizzati. La domanda, infatti, è la seguente: come fa il soggetto / utente interessato a esercitare tali diritti in un sistema decentralizzato, in cui i dati non sono cancellabili e, inoltre, sono anche pubblici e fruibili da chiunque? M. Seghesio, *Blockchain and Privacy*, *cit.*, 145, nota 51.

[73] J. Slaby, *Backups and the GDPR "right to be forgotten": Recommendations*, Acronis, 2018. Disponibile al sito https://www.acronis.com. Consultato il 08 giugno 2022.

[74] S. Brakeville & B. Perepa, *Blockchain basics: Introduction to distributed ledgers - Get to know this game-changing technology and how to start using it*, IBM Developer, 2018. Disponibile al sito https://developer.ibm.com/tutorials/cl-blockchain-basics-intro-bluemix-trs/. Consultato il 08 giugno 2022. In particolare, gli autori sottolineano la natura distribuita della *blockchain* affermando che si tratta di un «database that is shared, replicated, and synchronized among the members of a decentralized network. The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network. Participants in the network govern and agree by consensus on the updates to the records in the ledger. No central authority or third-party mediator, such as a financial institution or clearinghouse, is involved. Every record in the distributed ledger has a timestamp and unique cryptographic signature, thus making the ledger an auditable, immutable history of all transactions in the network». *Ibid.*

[75] A. Towers, *Blockchain Resolution Passed by EU Parliament but GDPR Could Be Weak Link*, William Fry, 2018. Disponibile al sito https://williamfry.com. Consultato il 08 giugno 2022.

[76] In particolare, l'aspetto della pseudonimizzazione dei dati personali (ossia «data can no longer be attributed to a specific individual without the use of additional information» Art. 4, no. 5, GDPR) è specificamente regolato dal GDPR ed è soggetto alla condizione che le informazioni aggiuntive siano «conservate separatamente» e soggette a misure tecniche e organizzative atte a garantire la non attribuzione a persona identificata o identificabile.

Con riferimento, per converso, ai potenziali punti di convergenza tra il GDPR e la tecnologia *blockchain*, va evidenziato come quest'ultima possa anche essere utilizzata in un modo tale da facilitare la protezione dei dati personali[77].

In particolare, ciò è vero perché questa tecnologia garantisce la scissione dei dati dall'identità individuale e la minimizzazione dei dati (ovvero la condivisione dei soli dati inevitabili).

Lo stesso Regolamento prevede che, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, vi è la possibilità che i dati personali possono essere conservati per periodi più lunghi rispetto a quanto acconsentito dal diretto interessato. Rimane, comunque, chiaro che la definizione stessa di pubblico interesse è quanto mai generica.

Più concretamente, i problemi legati alla *privacy* derivanti dalle caratteristiche proprie della *blockchain* possono essere mitigati dalla crittografia *end-to-end*, richiedendo chiavi private e pubbliche e, contestualmente, trovando alternative valide alla cancellazione dei dati[78].

[77] J. SLABY, *Backups and the GDPR*, *cit.*

[78] Anziché utilizzare un'unica chiave per la crittografia e la decrittografia, quindi, vengono utilizzate chiavi separate (una chiave pubblica e una privata, appunto), in modo tale da consentire agli utenti di inviare la propria chiave pubblica a chiunque, senza preoccuparsi che qualcun altro possa accedere alla propria chiave privata. Con riferimento all'aspetto dell'anonimato, si veda G. RESTA, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, in *Dir. Infor.*, 2014, 171.