LUISS

Dipartimento di GIURISPRUDENZA

Cattedra DIRITTO PRIVATO 2

La *blockchain* e la tutela dei dati personali

Relatore

Prof. Roberto Carleo

Correlatore

Prof. Silvio Martuccelli

Maria Cristina Galluccio

Matricola n. 135083

Anno Accademico 2019/2020

INDICE

INTRODUZIONE

Oggetto del presente lavoro di tesi è la disamina del rapporto intercorrente tra la tutela della *privacy* e la nuova tecnologia *blockchain*. La ragione di scelta di tale tematica risiede nella volontà di affrontare un argomento che viene costantemente in rilievo alla luce dei continui ed incessanti progressi che la tecnologia informatica comporta quotidianamente.

Invero, il contributo intende esaminare il rapporto complesso e affascinante che lega *blockchain* e diritto, mettendo in luce il quadro giuridico di riferimento ed esaminando alcuni profili particolarmente significativi, relativi all'applicazione di tale tecnologia nei vari settori di operatività dell'individuo, evidenziando, soprattutto, le varie questioni che possono insorgere nel momento in cui si tratta di far rispettare la normativa in materia di tutela dei dati personali nelle diverse attività poste in essere nell'ambito stesso della *blockchain*.

In via generale, l'analisi intende affrontare aspetti problematici dell'interazione tra la *blockchain* e l'ordinamento giuridico, come la validazione temporale dei documenti informatici, alcune applicazioni significative, nello specifico gli *smart contracts*, e profili di interazione con normative a tutela di diritti, in particolare la disciplina in materia di *Data Protection*.

Orbene, alla luce di quanto espresso in premessa, la disamina giuridica della *blockchain* deve necessariamente partire dall'oggetto della regolazione, dalla conoscenza di ciò che si vuole disciplinare e, pertanto, dalle caratteristiche tecnologiche, anche al fine di valutare la riconducibilità alle categorie giuridiche esistenti. L'osservazione della tecnologia *blockchain* è necessaria perché proprio in alcune caratteristiche emergono aspetti che concretizzano criticità per il diritto statuito e le norme esistenti.

Per questa ragione, nel primo capitolo, si renderà senz'altro utile alla comprensione del nostro discorso illustrare, a grandi linee, le caratteristiche architetturali della tecnologia *blockchain*, e delle sue componenti informatiche, nei

limiti di quanto necessario per procedere alla disamina delle problematiche giuridiche già oggetto di vivaci dibattiti e tentare di tracciare, *de iure condito*, la cornice normativa entro la quale si collocherebbe tale nuova tecnologia.

La prima considerazione che darà avvio alla trattazione, in particolare, è quella per cui la nuova tecnologia ha posto il giurista dinanzi a fenomeni del tutto nuovi, che gli hanno imposto e continuano ad imporgli costanti confronti, al fine della loro comprensione e della loro catalogazione nelle tradizionali – o nelle nuove – categorie civilistiche. Tra queste rientra senz'altro la *blockchain*, quale *species* del più ampio *genus* delle *distributed ledger technologies*, la quale si configura come una "catena di blocchi", dal momento che i dati, inseriti per mezzo di crittografia asimmetrica, sono allocati in blocchi, accompagnati da *hash* e validazione temporale, tra loro concatenati attraverso il richiamo dell'*hash* del blocco precedente in quello successivo: da questo aspetto deriva la caratteristica dell'immutabilità unilaterale. Ogni nuovo blocco è validato da alcuni nodi (i c.d. *miners*) per mezzo della risoluzione di un problema matematico, che vale una ricompensa, con un meccanismo che serve a incentivare la corretta validazione dei blocchi.

In via del tutto introduttiva, quindi, la *blockchain* può essere assimilata a un registro o a un libro mastro digitale, che conserva in modo immutabile la memoria storica delle transazioni avvenute e in cui, in modo distribuito e paritetico, ciascun partecipante dispone di una copia di ciascuna operazione, garantendo così sicurezza e resistenza rispetto a potenziali attacchi.

Il fenomeno, dunque, sarà esaminato alla luce del quadro giuridico europeo e italiano di riferimento e particolare attenzione sarà riservata ai c.d. "*smart contracts*", i quali hanno acquisito rilevanza con l'avvento della *blockchain*, grazie alla possibilità di garantire l'esecuzione del contratto indipendentemente dal volere delle parti coinvolte nel contratto. Si tratta di una nuova modalità di manifestazione del consenso, che si aggiunge a quella del contratto telematico e a quella del contratto c.d. cibernetico. Emergerà, infatti, dall'analisi condotta, che lo *smart contract* è uno strumento tecnologicamente avanzato e versatile a disposizione delle parti, che possono servirsene, nel contesto di un rapporto contrattuale, per finalità diverse: come mero veicolo di scambio delle dichiarazioni negoziali, come si

farebbe con una *e-mail* certificata; come mezzo di attuazione del contratto concluso in forma "tradizionale"; ovvero come fonte esso stesso del vincolo negoziale, rendendo quindi lo *smart contract* il "contratto".

Nel secondo capitolo, invece, l'attenzione sarà posta sulla lunga evoluzione che la tutela della *privacy* ha avuto nel corso del tempo, la quale è venuta modificandosi proprio in relazione al grande sviluppo che si è avuto nel processo tecnologico. In particolare, il capitolo prenderà avvio con la definizione del concetto di "diritto all'identità personale", che nell'era di *Internet* ha conosciuto l'ulteriore declinazione in diritto alla c.d. "identità virtuale", valutando in che modo l'ordinamento è riuscito ad apprestare idonea tutela.

Successivamente, si passerà all'esame del concetto di "dati personali" nella società dell'informazione per ricostruire l'origine del concetto di "*Privacy*" e la sua tutela nell'era digitale, analizzando il contributo dato in ordine a tale definizione da parte della dottrina e della giurisprudenza nazionali, nonché dalle fonti comunitarie.

Il terzo capitolo, infine, sarà interamente deputato all'analisi del difficile rapporto intercorrente tra la tecnologia *blockchain* e il c.d. Regolamento *Data Protection*. Invero, tutte le caratteristiche delineate nel primo capitolo in merito alla blockchain verranno messe a confronto con le nuove disposizioni regolamentari, al fine di valutare se le stesse possano o meno conciliarsi con i principi fissati nel GDPR, direttamente applicabile in tutti gli Stati membri, e con le norme contenute nel codice della *privacy*, recentemente adeguato al citato Regolamento, con il d.lgs. 10 agosto 2018, n. 101. Infatti, in tali disposizioni si afferma che il trattamento dei dati personali deve essere lecito, equo e trasparente; deve essere limitato allo scopo specifico per il quale sono stati originariamente raccolti; è possibile raccogliere solo i dati assolutamente necessari allo scopo specifico (c.d. minimizzazione dei dati); i dati devono essere accurati e aggiornati, non devono essere conservati più a lungo del necessario e devono essere elaborati in modo sicuro (integrità e riservatezza).

Partendo, dunque, dalla definizione di "dato personale" contenuta nel Regolamento, si valuterà la natura di "dato personale" delle informazioni immesse nella *blockchain*, ancorché cifrate tramite la funzione *hash* e il sistema della crittografia asimmetrica, al fine di comprendere se tali attività possano o meno ritenersi conformi alle disposizioni regolamentali. I sistemi *blockchain*, infatti, sono

una tecnica di pseudonimizzazione che consente di trattare le informazioni di un soggetto in modo tale da impedirne l'identificazione. I dati immessi nella *blockchain* sono, dunque, dati pseudonimizzati, considerati dal Regolamento come informazioni su una persona fisica identificabile, poiché ancorché non direttamente riconducibili a una persona fisica, lo possono essere con l'utilizzo di ulteriori informazioni.

È pur vero che alcuni dei principi stabiliti dal Regolamento trovano sicura tutela nella *blockchain*, se si considera che tale tecnologia, è decentralizzata e distribuita e questo rende molto più difficile un attacco di *cybercrime*; le informazioni sulle transazioni, quali l'identità dei soggetti e gli altri dati personali, sono, come detto, pseudonimizzate, ancorché pubbliche e, quindi, noti agli altri nodi; la crittografia utilizzata, in linea di principio, garantisce un metodo piuttosto sicuro per archiviare e gestire le informazioni.

Vi sono, tuttavia, come vedremo nello specifico nel corso della parte finale della trattazione, altri principi fissati nella normativa europea che difficilmente potranno essere rispettati, come quello che sancisce il diritto alla cancellazione dei dati personali (c.d. diritto all'oblio) o anche alla loro rettifica, stante il carattere immodificabile della *blockchain*.

CAPITOLO PRIMO

La tecnologia *blockchain*

SOMMARIO: 1. La tecnologia informatica ed il diritto. – 1.1. (*Segue*) Il ruolo del giurista. – 1.2. (*Segue*) Il giurista e la tecnologia *blockchain*. – 2. La nuova tecnologia della *blockchain*. – 2.1. Le origini storiche del sistema della *blockchain*. – 2.2. La *blockchain*: cos'è e come funziona. – 2.3. Le caratteristiche della *blockchain*. – 2.4. Le tipologie di *blockchain*: pubbliche, ibride e private. – 2.5. (*Segue*) La formazione del consenso nell'ambito della *blockchain*. – 3. Profili giuridici: il quadro europeo e italiano di riferimento. – 4. La *blockchain* ed i c.d. "*Smart Contracts*". – 4.1. (*Segue*) Il funzionamento dello *smart contract*. – 4.2. (*Segue*) La qualificazione giuridica degli *smart contracts*.

1. La tecnologia informatica ed il diritto.

L'evoluzione tecnologica sviluppatasi nel corso degli anni ha determinato un'incidenza di forte impatto sulla società umana comportando cambiamenti sociali, economici e culturali; invero, il grande sviluppo dell'informatica e delle tecnologie di comunicazione mediante l'utilizzo della rete *internet*[1] ha prodotto dei

[1] Internet nasce come ARPANet – dal nome dell'agenzia di ricerca americana che l'aveva progetta, *Advanced Research Project Agency* – nel 1969 con l'obiettivo di realizzare un flessibile strumento di comunicazione adatto a garantire il collegamento tra strutture militari, anche in caso di interruzioni delle linee principali di comunicazione. Cfr. sul punto APARO A., *Il libro delle reti*, Roma, 1995, *passim*.

profondi mutamenti[2], senza dubbio nei rapporti sociali ed economici, ma anche e soprattutto giuridici[3], introducendo nuove sfide per il legislatore e per i giuristi che con tali novità hanno dovuto costantemente confrontarsi[4], posto che il diritto rappresenta lo strumento principale di regolazione non solamente dei comportamenti, delle relazioni e delle attività, ma anche di bilanciamento di interessi, di tutela dei diritti e di soluzione dei conflitti[5].

Occorre, infatti, considerare che nella società contemporanea, l'articolata diffusione delle nuove tecnologie ed il progressivo accrescimento del loro impiego nell'attività giuridica di tutti i giorni ha condotto il diritto a dialogare con altre regole, in specifico con la c.d. *lex informatica* o *digitalis*, le regole informatiche, ossia le regole applicate dal "codice" informatico: il codice giuridico è chiamato a interagire con quello algoritmico per dare un'efficace disciplina al fenomeno che è in costante espansione in ogni ambito del diritto[6].

---

[2] Scrive BORRUSO R., *Computer e diritto*, tomo II, Milano, 1988, p. 41: "*l'energia elettrica – e più precisamente il flusso degli elettroni – è il nuovo mezzo di scrittura dell'umanità: il nuovo inchiostro di cui l'uomo si serve. Le memorie elettriche o elettroniche […] non sono altro che la nuova carta, cioè il nuovo supporto su cui l'uomo scrive con il nuovo inchiostro. […] i bit non sono altro che il nuovo alfabeto universale ed internazionale di cui l'uomo può servirsi per esprimere qualsiasi opera del pensiero*".

[3] Sottolinea come la contrattazione abbia subito notevoli cambiamenti in relazione soprattutto ai progressi tecnologici che hanno consentito nuove tecniche di comunicazione a distanza, MASTRORILLI D., *Contrattazione a distanza. Disciplina consumeristica e di settore*, Bari, 2011, pp. 13 ss. Cfr., altresì, IRTI N., *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, 2006, p. 187, il quale ha sostenuto che "la storia del contratto non può separarsi dalla storia delle tecnologie" attraverso cui possono delinearsi e svolgersi i rapporti di scambio.

[4] Certamente non può trascurarsi la considerazione per cui il fenomeno digitale ha invaso anche gli spazi della pubblica amministrazione, i quali da sempre si sono connotati per essere maggiormente restii all'innovazione tecnica. Proprio in virtù di tale ragione, si sono nel corso del tempo avviate delle iniziative tese proprio ad incentivare il ricorso alla tecnologia nell'ambito delle procedure interne ai sistemi pubblici. Ne è un esempio l'emanazione del Codice dell'amministrazione digitale con il d.lgs. n. 82/2005; non solo, ma anche gli interventi della Presidenza del Consiglio dei Ministri, dipartimento per le innovazioni e le tecnologie, con la sempre frequente pubblicazione delle "linee guida in materia di digitalizzazione dell'amministrazione". Si tratta di iniziative dirette ad incentivare lo sviluppo e l'erogazione di servizi *on-line* per cittadini e imprese; l'accessibilità dei siti *Internet* della pubblica amministrazione; la trasparenza dell'azione pubblica attraverso l'adozione del protocollo informatico; l'efficienza delle amministrazioni attraverso l'utilizzo della posta elettronica e del documento elettronico; la distribuzione ai dipendenti pubblici di carte elettroniche (*smart cards*) multiservizi; la sicurezza delle tecnologie dell'informazione e della comunicazione; lo sviluppo delle competenze attraverso la formazione *on-line* (*e-learning*). Si tratta sostanzialmente di interventi che mirano ad uno sviluppo sempre maggiore della "società dell'informazione".

[5] Cfr. FAINI F., *Blockchain e diritto: la «catena del valore» tra documenti informatici, smart contracts e data protection*, in *Responsabilità Civile e Previdenza*, fasc.1, 2020, p. 297.

[6] Cfr. GIULIANO M., *La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio*, in *Diritto informatico e dell'informatica*, 2018, pp. 989 ss.

La *lex informatica*, invero, proprio per l'aumentare della complessità dei rapporti intersoggettivi che si attuano con le nuove tecnologie, incide in misura preponderante sui comportamenti umani, abilitando o meno azioni e interazioni, facilitandole e collegando ad esse effetti e conseguenze[7]. Proprio per sottolineare l'incidenza del codice informatico nel campo giuridico, in dottrina si è coniata la locuzione "*code is law*"[8], secondo cui con l'avanzare della tecnologia digitale non è più principalmente la legge a regolare il comportamento degli utenti bensì è il codice *software* che ne plasma sempre più diritti ed oneri, basandosi su una sorta di *lex informatica* costituita dagli accordi che vengono fatti accettare per l'utilizzo dei servizi, ma anche dalle regole che vengono sempre più incorporate nel codice, ma con una precisazione: *code is law* solo quando il diritto, assolvendo alla sua funzione preventiva di regolazione, incorpori nel linguaggio macchina il rispetto dei principi e delle norme[9].

Orbene, posto che l'uomo disciplina i comportamenti e le relazioni dei consociati mediante lo strumento del diritto, di conseguenza, l'evoluzione tecnologica, che caratterizza profondamente la società contemporanea, ha bisogno di essere governata dalla scienza giuridica. In altre parole, il diritto è chiamato a governare la tecnologia e quindi anche le sue espressioni – quali la c.d. "*blockchain*" – ma, nel farlo, il giurista deve essere in grado di raggiungere un difficile equilibrio, che sia capace di non limitare lo sviluppo tecnologico, ma parimenti riesca a non determinare la prevalenza della tecnologia sulla regolazione giuridica[10].

Di talché, nel disciplinare la tecnologia, il diritto deve intervenire per bilanciare efficacemente la garanzia del rispetto dei principi dell'ordinamento e la

---

[7] Cfr. SARTOR G., *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, II ed., Torino, 2010, pp. 37 ss.
[8] Cfr. LESSIG L., *Code and Other Law of Cyberspace*, New York, 1999.
[9] Cfr. FAINI F., *Blockchain e diritto: la «catena del valore» tra documenti informatici, smart contracts e data protection*, cit., p. 297.
[10] Cfr. SARTOR G., *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, cit., pp. 37 ss.; FINOCCHIARO G., *Riflessioni su diritto e tecnica*, in *Diritto informatico e dell'informatica*, 2012, pp. 831-840, la quale ritiene che "il diritto (o la politica, in taluni casi) debba stabilire gli obiettivi (se non addirittura i valori) e che la tecnica debba essere il mezzo per raggiungerli. La tecnica deve essere etero-diretta o quanto meno dall'esterno controllata"; CORASANITI G., *Il diritto nella società digitale*, Milano, 2018, p. 15, secondo cui il diritto "ha sempre fatto uso, il miglior uso possibile, delle tecnologie disponibili per affermarsi e per assicurare e quindi salvaguardare adeguatamente gli spazi di libertà e di giustizia delle società umane".

tutela dei diritti previsti nei settori che sono interessati dall'evoluzione tecnologica[11], tenendo in considerazione il fatto che il "fenomeno *Internet*" non costituisce un nuovo "ambiente", un luogo fisico in cui è possibile navigare[12], ma è un mezzo di comunicazione: ed è, per di più, un mezzo di comunicazione che per sua natura rende assai difficoltosa la collocazione geografica dei soggetti che di esso si servono per comunicare[13].

1.1. (*Segue*) Il ruolo del giurista.

Il tema di *Internet* rappresenta per il giurista fonte di forti sollecitazioni, ancor più ove lo si affronti nell'ottica dei cambiamenti che il suo avvento ha determinato in ogni ambito della vita giuridica[14]. D'altro canto, si tratta di un fenomeno nuovo, che ha imposto, anzitutto, al giurista il dovere di conoscerlo, di individuare e di studiare le caratteristiche essenziali, di comprenderlo, al fine precipuo di valutare se esso possa essere ricondotto o meno alle tradizionali categorie già esistenti nell'ordinamento giuridico, e al fine di fornirne una sua qualificazione[15], atteso che si tratta certamente, come sottolineato in dottrina, di un fenomeno "*né transitorio, né meramente accessorio*"[16]. Al contrario, esso appare come una opportunità da sfruttare da parte di imprese, cittadini ed istituzioni, nell'ambito della realizzazione di uno "spazio senza frontiere"[17].

Lo sviluppo di *Internet* ha, infatti, permesso il passaggio da una funzione meramente passiva, ove gli utenti si limitavano a visionare e recepire le informazioni che venivano loro fornite, ad una nuova situazione nella quale, invece,

---

[11] Cfr. RODOTÀ S., *Intervista su privacy e libertà*, a cura di Conti, Roma-Bari, 2005, pp. 12 ss.
[12] Cfr. FINOCCHIARO G., *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su Internet*, in *Contratto e Impresa in Europa*, 2001, pp. 571 ss.
[13] Scrive BALLARINO T., *Internet nel mondo della legge*, Padova, 2007, p. 17: "Internet non è un'entità fisica o tangibile, ma piuttosto una gigantesca rete che interconnette un numero infinito di gruppi più ristretti di reti informatiche collegate tra di loro".
[14] Cfr. PICA G., voce *Internet (diritto penale)*, in *Digesto delle discipline penalistiche*, Milano, 2004, pp. 425-483.
[15] Cfr. FINOCCHIARO G., *Il contratto nell'era dell'intelligenza artificiale*, in *Rivista Trimestrale di Diritto e Procedura Civile*, fasc.2, 2018, p. 441.
[16] Cfr. CLARIZIA R., *Informatica e conclusione del contratto*, Milano, 1985, p. 14.
[17] Si vedano Secondo e Terzo Considerando della Direttiva sul commercio elettronico, n. 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000, pubblicata nella Gazzetta Ufficiale della Comunità Europea del 17 luglio 2000.

vi è una crescente interazione con la rete, nella quale le applicazioni *web* interattive rendono più semplice ed agevole la condivisione e lo scambio delle informazioni. Basti pensare, per fare un esempio, ai procedimenti di registrazione e di utilizzo dei *social network* o delle piattaforme che erogano i più svariati servizi dove ciascun utente inserisce i propri dati a fronte del rilascio di credenziali di accesso – ad esempio *username* e *password* –, che costituiscono proprio la rappresentazione biunivoca tra l'utente e i suoi attribuiti identificativi[18].

Nello specifico, l'identità digitale rappresenta il risultato di un costante processo di arricchimento, che contribuisce a realizzare un patrimonio informativo formato "non solo su ciò che è e fa chi ne dispone, ma anche sulle relazioni e reazioni che i suoi atti sono in grado di generare"[19]. Ciò fa sì che l'identità digitale possa via via assumere diverse forme[20] che, non necessariamente, ma spesso, si allontanano dall'identità personale del soggetto cui appartiene, sia per il tramite di informazioni che altri elaborano sullo stesso, sia per la veridicità di informazioni che lo stesso soggetto comunica alla rete. Questo, ovviamente, non sempre può accadere, posto che vi sono anche dei servizi *on line* che per poter essere fruiti necessitano di informazioni vere e precise sull'identità personale di un soggetto e certificate da altri soggetti a tale scopo autorizzati.

Al giurista, dunque, è richiesto di non trascurare tale fenomeno sociale, che muta nel corso del tempo in quanto "prodotto e contemporaneamente motore di cambiamenti culturali, economici, sociali e politici"[21]. Nella ricerca dei mezzi di tutela da apprestare alle molteplici e complesse istanze che l'individuo nella sua dimensione digitale avanza, il giurista deve porsi nella condizione di recepire il

---

[18] Cfr. ROVEGNO A.O., *Identità digitale: tra esigenze di condivisione e necessità di tutela*, in *Cyberspazio e Diritto*, 2013, fasc. 3, pp. 403-423.

[19] Cfr. GIGLIO V., *Identità e profilazione digitale: i rischi dei Big Data*, in *Filodiritto*, 22 novembre 2016, pp. 1-8.

[20] In particolare, ROOSENDALE A., *Digital personae and profiles as representations of individuals*, in *Privacy and identity management for life*, 2010, *passim.*, identifica il concetto di persona digitale in tre forme diverse: una forma Progettata, una Imposta ed una Ibrida. La forma progettata è quella che l'individuo sceglie, forma e rappresenta per mezzo dei contenuti che immette, come, ad esempio, nel caso di una *homepage* di un sito personale; la forma imposta è l'identità creata da enti esterni, attraverso le elaborazioni di dati che ci riguardano, come nel caso della determinazione del merito creditizio da parte delle società di *rating*; la forma ibrida è la rappresentazione creata dal *web* 2.0 e dalle sue connessioni sociali, specialmente attraverso la profilazione dei dati raccolti nei siti che si visitano o ai quali ci si registra, come nel caso dei *social network*.

[21] PAROLA L., MERATI P., GAVOTTI G., *Blockchain e smart contract: questioni giuridiche aperte*, in *Contratti*, 2018, fasc. 6, pp. 681 ss.

cambiamento e deve contribuire alla creazione delle nuove disposizioni regolatrici atte a fornire soluzioni nuove che siano al passo con la tecnologia e che allo stesso tempo non la finiscano con il cristallizzare tale fenomeno entro gli angusti limiti delle categorie settoriali. Il giurista, infatti, "non può – e non deve – rinunciare al proprio ruolo, alla propria presenza, al proprio operare per conoscere i fenomeni, valutare la concreta rilevanza e qualità degli interessi in gioco e individuarne le opportune discipline e regole"[22].

La rete, del resto, si è già pienamente rivelata come un luogo profondamente concreto e capace di accogliere nel suo ambito le varie esigenze della vasta gamma di utenti che sempre di più fanno ricorso al suo tramite per porre in essere le loro attività[23]. Tuttavia, queste stesse caratteristiche debbono mettere in guardia il giurista e gli operatori giuridici in genere dal ritenere sicuramente sufficiente per la comprensione del fenomeno in questione il ricorso alle tradizionali categorie concettuali, dovendosi, invece, impegnare in uno sforzo ricostruttivo i cui capisaldi teorici sono verosimilmente in gran parte in via di continua formazione e cambiamento[24].

Invero, basti pensare ai vari nuovi beni e nuovi interessi giuridicamente ed economicamente rilevanti che l'incessante evoluzione tecnologica ha realizzato e che, inevitabilmente, lo strumento giuridico non ha potuto ignorare; ha anche aperto nuovi orizzonti impensabili fino a qualche anno fa nel mondo della comunicazione e della trasmissione di dati e di informazioni di ogni genere[25].

Orbene, tutti questi aspetti, connessi all'incessante sviluppo del fenomeno informatico, lungi dall'essere "una sorta di *far west* allergico ad ogni regola"[26],

---

[22] Cfr. GABRIELLI E., RUFFOLO U., *Intelligenza Artificiale e diritto*, in *Giurisprudenza Italiana*, Luglio 2019, p. 1657.

[23] Come ha scritto BRUGALETTA F., *Internet per giuristi*, 4a ed., Napoli, 2003, 9, la c.d. "rete delle reti" è "un *medium* persuasivo in grado di influenzare le stesse relazioni personali ed il modo di pensare".

[24] Cfr. COSTANZO P., voce *Internet (diritto pubblico)*, in *Digesto delle discipline pubblicistiche*, Aggiornamento, Torino, 2000, pp. 347 ss.

[25] Cfr. HANCE O., *Internet e la legge*, Milano, 1996, p. 3. In particolare l'Autore scrive: "Internet è il precursore delle autostrade dell'informazione".

[26] Cfr. SIROTTI GAUDENZI A., *Proprietà intellettuale e diritto della concorrenza*, Padova, 2010, p. 56. Tuttavia, la giurisprudenza nazionale è giunta in talune occasioni a ritenere la rete Internet come una sorta di "nuovo ordinamento" caratterizzato da proprie peculiarità. Ad esempio, nel 2001 il Tribunale di Firenze ha affermato che "il mondo della comunicazione telematica […] costituisce indubbiamente un ordinamento particolare, caratterizzato da proprie regole tecniche, in relazione al quale pone il problema della regolamentazione giuridica da parte dei singoli Stati, e cioè, dei vari

determinano, al contrario una costante necessità di adeguamento della normativa, la quale deve essere in grado di tener conto di tutte le novità che tali sistemi introducono nell'instaurazione e nel funzionamento dei rapporti interpersonali[27].

1.2. Il giurista e la tecnologia *blockchain*.

Come sinora ribadito, dunque, la tecnologia digitale ha influito in maniera decisiva sul modo in cui i consociati hanno regolato le proprie relazioni e, quindi, indirettamente, sul diritto che governa la società[28].

Il *cyberspazio* (o *cyberspace*) – ossia lo spazio virtuale all'interno del quale si collocano la *blockchain* e gli *smart contracts* – è governato da un proprio linguaggio, c.d. codice informatico, che lo definisce e lo regolamenta, e dal quale discende una delle tante architetture possibili, così come accade nello spazio reale, in cui il complesso delle norme giuridiche dettate dal legislatore definiscono, in un determinato territorio, un dato ordinamento giuridico[29].

Il codice informatico – o *lex informatica* – costituisce, quindi, un sistema di regole tecniche che si pongono in posizione parallela rispetto a quelle giuridiche, in cui il programmatore del codice detiene il potere regolatorio dello spazio virtuale, allo stesso modo del legislatore, con l'unica differenza dell'assenza, nello spazio virtuale, di limiti territoriali e di frontiere fisiche, posto che è ben possibile che persone situate in luoghi geograficamente anche molto distanti possono agevolmente entrare in contatto in tempo reale. Appare, pertanto, necessario conoscere le "regole tecniche" che governano la tecnologia esaminata, poiché, come detto, influenzano e limitano l'efficacia coattiva della norma a regolare le modalità di svolgimento delle relazioni che si svolgono in essa[30].

---

ordinamenti con i quali quello telematico viene ad essere in relazione". Cfr. Tribunale Firenze, sentenza del 7 giugno 2001, in *Foro toscano - Toscana Giurisprudenza*, 2002, p. 105.

[27] Cfr. CLARIZIA R., *I contratti informatici*, cit., p. 7.

[28] Cfr. PASCUZZI G., *Il diritto dell'era digitale*, Bologna, 2002, pp. 61-66. In particolare, l'Autore sottolinea il fatto che la tecnologia, da un lato, ha determinato il verificarsi di nuove situazioni che possono minare la riservatezza degli individui, dall'altro ha, tuttavia, predisposto anche dei rimedi da utilizzare per la difesa dei propri dati personali.

[29] Cfr. CORASANITI G., *Il diritto nella società digitale*, cit., passim.

[30] Cfr. sul punto, in particolare, TOSI E., *Contratti informatici, telematici e virtuali*, Milano, 2010, pp. 14 e ss.

In particolare, l'avvento della tecnologia *blockchain* – che la dottrina ha definito "*disruptive*"[31] – ha, senza dubbio, contribuito in misura preponderante nel generare un mutamento delle relazioni umane, che, ovviamente, si riverbera sul diritto, influenzandolo, soprattutto per quanto riguarda la sua funzione di strumento di tutela e di soluzione dei conflitti. Invero, all'interno di quello che possiamo definire come il "mondo virtuale" sorge la necessità di proteggere tutte le varie proiezioni della persona: il soggetto, infatti, costruisce una propria identità digitale, ossia la rappresentazione virtuale della sua propria identità di persona, la quale viene utilizzata quale mezzo di connessione tra il reale ed il digitale[32].

Orbene, la tecnologia dell'informazione ha avuto un ruolo fondamentale nella trasformazione del modo di operare delle aziende, posto che essa ha consentito di automatizzare le varie operazioni manuali e di processare l'informazione più velocemente. Non solo, ma anche creato nuove forme di comunicazione e altri metodi di lavoro che le imprese utilizzano durante l'elaborazione delle informazioni finanziarie e di *business*.

Cambia anche il modo di intendere il mercato, il quale da luogo ideale entro il quale avvengono, tendenzialmente in autonomia, gli scambi tra le parti, diventa ora un prodotto dell'ordinamento giuridico, non potendo esistere, né potendo gli individui operare in esso, senza regole giuridiche che lo ordinino[33], posto lo sviluppo di nuovi modelli di *business* prima inimmaginabili, di cui l'ordinamento non può non tenere conto. Va da sé che il giurista non può intervenire *ex ante* e in astratto fenomeni innovativi dirompenti, come è stato *Internet* 30 anni fa e come è adesso la tecnologia *blockchain* e le sue applicazioni nelle relazioni sociali. E "questo è tanto più necessario in quanto l'innovazione scientifica e tecnologica si fa portatrice di un mutamento incessante che non può essere governato attraverso il tradizionale inseguimento legislativo. È indispensabile, quindi, 'privilegiare' strumenti 'prospettici', quali sono appunto quelli legati a una normativa per princìpi, mentre la costruzione di una disciplina affidata a fattispecie chiuse

[31] Cfr. BOWER J.L., CHRISTENSEN C.M., *Disrupting Technologies: Catching the Wave*, in *Harvard Business Review*, fasc. I, 1995, p. 10, il quale definisce la tecnologia *blockchain* "*distruptive*" perché "*bring to a market a very different value proposition than had been available previously*".
[32] Cfr. GIULIANO M., *La Blockchain e gli Smart Contracts nell'innovazione del diritto nel terzo millennio*, cit., p. 989.
[33] Cfr. CATAUDELLA A., *L'uso abusivo di principi*, in *Rivista di diritto civile*, 2014, fasc. 4, p. 747.

presuppone un diritto che interviene alla fine di un ciclo, che scende alla sera, per selezionare e razionalizzare interessi e situazioni ormai consolidati"[34]. Si è, dunque, aperta la via delle c.d. "*sunset rules*", ossia delle norme destinate a tramontare e ad essere sostituite ad una scadenza predeterminata, prevedendo così un obbligo del legislatore (o di altri soggetti) di intervenire nuovamente per disciplinare la materia allo stadio in cui di volta in volta si trova[35].

In altre parole, compito del giurista diventa quello di non permettere che il diritto si lasci piegare dalle esigenze della tecnica lasciando che questa imponga la regolazione, ma, al contrario è necessario che le nuove tecnologie siano effettivamente vagliate dal giurista affinché egli possa intervenire per plasmare il diritto esistente rendendolo conforme al nuovo che avanza, nel rispetto dei principi di ciascun ordinamento nel quale il fenomeno si colloca. Laddove le regole predisposte dall'ordinamento giuridico si rivelino inefficaci a disciplinare nuove forme di relazioni, soprattutto quando ci si trova di fronte a paradigmi del tutto nuovi, come nel caso dei rapporti dematerializzati eseguiti in una rete senza intermediari, e dove, oltre ai beni, è la stessa persona ad assumere un'identità virtuale, sarà compito del legislatore intervenire per adottare le più opportune soluzioni affinché l'individuo possa esplicare la propria attività in un contesto comunque garantito e regolato. È necessario, infatti, disciplinare i comportamenti e le attività al fine di non incorrere nell'errore di rendere tutto ciò che è tecnologicamente possibile, solo per questo, anche giuridicamente legittimo[36].

In uno scenario di questo tipo, ciò che il giurista è chiamato a fare è, dunque, raccogliere sistematicamente i fatti e studiare le pratiche mercantili, per ricondurle – laddove possibile – agli istituti giuridici esistenti e, in tal modo, individuarne la disciplina applicabile.

---

[34] Cfr. RODOTÀ S., *Tecnopolitica, la democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004, pp. 23 ss.

[35] Cfr. RODOTÀ S., *Tecnopolitica, la democrazia e le nuove tecnologie della comunicazione*, cit., passim.

[36] Cfr. GALIMBERTI U., *Psiche e techne: l'uomo nell'età della tecnica*, Milano, 1999, versione e-book. In particolare, l'Autore scrive: "Noi continuiamo a pensare la tecnica come uno strumento a nostra disposizione, mentre la tecnica è diventata l'ambiente che ci circonda e ci costituisce secondo quelle regole di razionalità che, misurandosi sui soli criteri della funzionalità ed efficienza, non esitano a subordinare le esigenze dell'uomo alle esigenze dell'apparato tecnico". Ne risultano così rivisti "i concetti di individuo, identità, libertà, spazio, tempo di cui si nutriva l'età umanistica e che ora, nell'età della tecnica, dovranno essere riconsiderati, dismessi o rifondati alle radici".

Questo vuol dire che il giurista deve mettersi nella prospettiva di accogliere le novità poste dalla tecnica, confrontandole con le categorie concettuali tradizionali, le quali devono fungere da strumento di sostegno per pervenire ad una regolamentazione effettiva del fenomeno[37], posto che di fatto, sovente, i classici criteri classificatori si rivelano insufficienti nel dare risposta alle istanze sociali di tutela e certezza del diritto nelle relazioni[38].

D'altro canto, un simile dibattito si era già sviluppato in dottrina con riguardo alla categoria dei contratti informatici[39], nell'accezione ampia di contratti di utilizzazione degli strumenti dell'informatica e di contratti di acquisizione, elaborazione e diffusione di dati a mezzo di strumenti informatici[40]; in particolare,

[37] Cfr. LIPARI N., *Le categorie del diritto civile*, Milano, 2013, p. 33.
[38] Cfr. FERRI G.B., *Le stagioni del contratto e il pensiero giuridico di G. Alpa*, in *Rivista di diritto commerciale*, 2013, p. 215.
[39] La dottrina in tema di evoluzione dei contratti informatici ha fornito contributi notevoli nel corso del tempo. È possibile individuare anche delle diverse fasi susseguitesi nel corso del tempo. In particolare, nella prima fase sono da segnalare gli studi di LOSANO M.G., *Il diritto privato dell'informatica*, Torino, 1986, pp. 18 e ss.; FROSINI V., *Informatica diritto e società*; Milano, 1988, p. 261; BORRUSO R., *Computer e diritto*, cit., p. 210 e ss.; ALPA G., *I contratti di utilizzazione del computer*, in *Giurisprudenza italiana*, 1983, IV, p. 42; CLARIZIA R., *Spunti per uno studio sui contratti di utilizzazione degli elaboratori*, in *Giurisprudenza italiana*, 1983, IV, p. 302 e CLARIZIA R.., *Informatica e conclusione del contratto*, cit.; MIRABELLI G., *Contratto tra terminali e documento elettronico*, in *Rivista notariato*, 1986, p. 120, di AA.VV., a cura di G. Alpa, V. Zeno-Zencovich, *I contratti di informatica: profili civilistici, tributari e di bilancio*, Milano, 1987. Nella fase successiva, che è, invece, quella più recente, è possibile menzionare i contributi di GAMBINO A., *L'accordo telematico*, Milano, 1997; TOSI E., *I contratti di informatica*, Milano, 1993, FINOCCHIARO G., *I contratti ad oggetto informatico*, Padova, 1993; FINOCCHIARO G., *I contratti informatici*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia*, diretto da F. Galgano, vol. XXII, Padova, 1997; SAVORANI G., *I contratti dell'informatica*, in *I contratti in generale*, a cura di G. Alpa, M. Bessone, Agg. 1991-1998, vol. II, Torino, 1999, p. 1433.
[40] In particolare, in dottrina, vi è chi (SGUERSO F., *Il contratto telematico. Le moderne tecnologie e il "vecchio" codice civile*, in *www.aicsweb.it/documenti/2012/*, p. 1) ha proposto la distinzione, nell'ambito della categoria generale dei contratti informatici, tra contratti digitali, quali contratti stipulati con firma elettronica; telematici, ossia quelli conclusi mediante strumenti telematici tra persone non fisicamente presenti; ed informatici, se aventi ad oggetto beni e servizi di tipo informatico. Altra parte della dottrina, invece, si è limitata ad individuare in generale la categoria dei contratti virtuali (cfr., tra gli altri, TOSI E., *Il contratto virtuale* (parte 1), in *Studium Juris*, 2008, p. 670, distinguendo fra virtualità in senso proprio – contratto stipulato dall'utente per il tramite di un sito *web* predisposto da un professionista – e senso improprio – ricomprendente anche la contrattazione via mail –. Secondo questo Autore, in particolare, il contratto virtuale in senso improprio contemplerebbe i contratti conclusi via mail). Secondo altri Autori, ancora, è possibile distinguere tra contratti a conclusione informatica (FUERGIUELE L., *I contratti a conclusione telematica*, in F. Bocchini, *Diritto dei consumatori e nuove tecnologie*, I, *Gli scambi*, Torino, 2002, pp. 145 ss.), ad oggetto informatico (FINOCCHIARO G., *I contratti ad oggetto informatico*, cit.; PICARO R., *I contratti ad oggetto informatico*, in F. Bocchini, *Diritto dei consumatori e nuove tecnologie*, I, *Gli scambi*, Torino, 2002, pp. 88 ss.), ad esecuzione informatica (PICARO R, *I contratti ad esecuzione informatica*, cit., pp. 207 ss.). Vi è infine chi propende per la categoria generale del contratto digitale (BIANCA M., *Istituzioni di diritto privato*, Milano, 2014, p. 406, il quale, escluso che si tratti di un nuovo tipo, definisce telematico il contratto stipulato con strumenti informatici).

ci si è chiesti se fosse opportuno procedere verso la creazione dogmatica di una nuova ed autonoma categoria contrattuale caratterizzata dall'avere ad oggetto beni o servizi dell'informatica[41]. Per una parte della dottrina – seppur minoritaria –, infatti, l'enucleazione di una categoria dei contratti di informatica servirebbe solamente per identificare un nucleo minimo di elementi giuridici, comuni alla categoria individuata, in grado di dotare di certezza e regolazione i rapporti che da essi sorgono[42]. Sulla questione la prevalente dottrina è, tuttavia, orientata nel senso di escludere che una particolare conformazione tecnologica ed economica dell'oggetto della prestazione possa, di per sé sola, legittimare la creazione di una categoria negoziale, posto che questo nuovo oggetto ben potrebbe essere ricompreso all'interno dei tradizionali schemi contrattuali senza perciò determinare un nuovo riferimento normativo[43].

Ad alimentare ancora di più il dibattito circa la corretta qualificazione giuridica del contratto informatico, si è posta la diffusione dei c.d. "*smart contracts*", o, per dirla con un'espressione italiana, "contratti intelligenti": come vedremo meglio nel prosieguo della trattazione, si tratta di algoritmi scritti e programmati per eseguire – o essere essi stessi – un accordo intercorso tra le parti di un rapporto – in modo automatico e indipendentemente da un intervento umano – nel momento in cui vengono realizzate le condizioni predefinite nel protocollo medesimo.

È una soluzione innovativa che, come sottolineato in dottrina, nasce "nella brillante commistione di principi e schemi di ragionamento afferenti aree tematiche rimaste in precedenza concettualmente distanti, vale a dire la crittografia, le reti distribuite *Peer-to-Peer* (p2p), gli algoritmi di consenso, la teoria dei giochi e la politica monetaria"[44].

---

[41] In particolare, propende in tal senso ZENO ZENCOVICH V., *Sul rilievo pratico o sistematico della categoria dei c.d. contratti di informatica*, in AA.VV., *I contratti di informatica. Profili civilistici, tributari e di bilancio*, a cura di Alpa G. e Zeno-Zencovich V., Milano, 1987, p. 32; GALGANO F., *La cultura giuridica italiana di fronte ai problemi informatici (considerazioni di sintesi)*, in AA. VV., *I contratti di informatica. Profili civilistici, tributari e di bilancio*, a cura di Alpa G. e Zeno-Zencovich V., Milano, 1987, pp. 373-375.

[42] Cfr. TRIPODI E.M., *Formulario dei contratti d'informatica e del commercio elettronico*, 3° ed., Roma, 2002, p. 5.

[43] Cfr. ALPA G., *Sulla qualificazione dei "contratti di informatica"*, in *Economia e diritto terziario*, Roma, 1989, p. 7.

[44] Cfr. RINALDI G., *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contratto e Impresa*, 2019, fasc. 1, p. 257.

Si tratta, dunque, di un istituto che coinvolge al contempo tanto elementi di diritto, quanto elementi dell'informatica, lasciando al giurista il delicato compito di intervenire per delineare il quadro normativo atto a regolare tutti questi comportamenti che sono possibili mediante il dispositivo tecnologico o, più in generale, mediante l'utilizzo dei nuovi strumenti informatici. Tuttavia, non si può certamente tralasciare la considerazione per cui proprio l'utilizzo di tali dispositivi digitali contribuisce in misura notevole anche al progresso giuridico, posto che impongono al legislatore di intervenire per regolamentare nuovi comportamenti tecnologicamente possibili, laddove non si possa ricorrere ai tradizionali schemi, i quali andranno, invece, opportunamente adattati al nuovo contesto socio economico. Ecco perché si rivela indispensabile conoscere le tecnologie al fine di individuare la regolamentazione atta a tener conto di tutte le potenzialità di intervento degli strumenti informatici[45].

2. La nuova tecnologia della *blockchain*.

La tecnologia *blockchain* nasce e si sviluppa rapidamente in combinazione con la diffusione delle c.d. *cryptovalute* e, più specificamente, del *bitcoin*. Essa, infatti, permette di registrare in modo sicuro e immodificabile i passaggi della moneta tra gli utenti, mediante la creazione di registri criptati, condivisi e aggiornati in tempo reale[46]. Questi registri rappresentano degli speciali *database*, condivisi,

[45] Cfr. GIULIANO M., *La Blockchain e gli Smart Contracts nell'innovazione del diritto nel terzo millennio*, cit., p. 989.

[46] La dottrina italiana in materia ha fornito notevoli contributi. Per citarne alcuni, cfr. BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto dell'informatica*, 2017, 1, pp. 27-54; FASSÒ F., *Il regime fiscale dei bitcoins secondo una recente (e unica) prassi amministrativa. Un passo avanti e un'occasione mancata*, in *Strumenti Finanziari e Fiscalità*, 2017, fasc. 3, pp. 105-113; CUCCURU P., *Blockchain ed automazione contrattuale. Riflessione sugli smart contract*, in *Nuova giurisprudenza civile*, 2017, fasc. 1, pp. 107-119; LEMME G., *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Rivista di diritto bancario*, 2016, 43, pp. 1 ss.; CAPAROGNA A., PERAINO L., PERUGI S., CECILI M., ZBOROWSKI G., RUFFO A., *Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione*, in *Diritto Mercato Tecnologia*, 2015, fasc. 3, pp. 32-74; MONTALCINI C., SACCHETTO F., *Bitcoin e criptovalute*, in *Diritto tributario telematico*, a cura di Montalcini e Sacchetto, Torino, 2017, p. 139-171; MANCINI N., *Bitcoin: rischi e difficoltà normative*, in *Banca impresa società*, 2016, fasc. 1, pp. 111-139; GASPARRI G., *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*,

che possono essere gestiti e modificati solo a certe condizioni, senza che vi sia un'autorità centrale a definire regole e permessi[47].

Si tratta, a ben vedere, di una tecnologia particolarmente versatile, essendo evidente la possibilità di usare i registri così congegnati anche per applicazioni diverse da quelle che riguardano la moneta digitale. Il dibattito dottrinario in merito si è rivelato sin da subito particolarmente animato ed eterogeneo: gli studiosi e le nuove imprese che si sono via via specializzate sull'utilizzo di questa tecnologia, hanno ritenuto che essa rappresentasse una vera rivoluzione, essendo insita in essa la capacità di introdurre nuovi modelli di *business*; in particolare, gli "*incumbent*", ossia le imprese, le istituzioni, le banche, hanno, invece, adottato un approccio senza dubbio più prudente, ma hanno comunque riconosciuto sin da subito il potenziale alla tecnologia, la quale avrebbe senz'altro potuto migliorare i *business model* che loro già utilizzano[48].

Le potenzialità della tecnologia *blockchain*, come nuova tecnologia informatica sono attualmente oggetto di discussione non solo nel campo delle criptovalute, ma anche in ambiti diversi, come per esempio nel settore della logistica, in quello della circolazione dei titoli e delle partecipazioni sociali, nonché in materia di proprietà industriale e intellettuale[49]. Soprattutto negli ultimi anni, sia in campo accademico che nel campo delle applicazioni pratiche, infatti, sono stati formulati vari suggerimenti e ipotesi in merito a come la tecnologia *blockchain* potrebbe essere utilizzata.

---

in *Il diritto dell'informazione e dell'informatica*, 2015, fasc. 3, pp. 415-442; VARDI N., *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin*, in *Il diritto dell'informazione e dell'informatica*, 2015, 3, pp. 443-456; GRECO G.L., *Monete complementari e valute virtuali*, in *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, a cura di Paracampo, Torino, 2017, pp. 197-216; DI SABATO D., *Gli smart contracts: robot che gestiscono il rischio contrattuale*, in *Contratto e Impresa*, 2017, fasc. 2, pp. 378-402.

[47] Cfr. DI PAOLA N., *Blockchain e Supply Chain Management*, Torino, 2018, pp. 69 ss.

[48] Cfr., in particolare, MEIJER D.B., *Consequences of the implementation of the Blockchain technology. Mater Thesis*, Delft University of Technology, 2017, passim.; NOWIŃSKI W., KOZMA M., *How Can Blockchain Technology Disrupt Existing Business Models?*, in *Entrepreneurial Business and Economics Review*, 5(3), 2017, pp. 173-188.

[49] Cfr. MOSCON V., *Tecnologie blockchain e gestione digitale del diritto d'autore e connessi*, in *Diritto Industriale*, 2020, fasc. 2, p. 137.

2.1. Le origini storiche del sistema della *blockchain*.

Se si volessero rintracciare, dal punto di vista storico, le origini del sistema della *blockchain*, ci si dovrebbe spostare sull'isola di Yap, in Micronesia, nel 500 d.C., ove si era andato progressivamente sviluppando un sistema di pagamento che per certi aspetti era molto simile a quello utilizzato oggi per la moneta virtuale. In particolare, per effettuare gli scambi a quell'epoca si utilizzava una moneta denominata "pietra Rai": si trattava di grandi dischi a forma circolare, perforati nel centro per permetterne il trasporto con l'utilizzo di pali, di dimensioni considerevoli, posto che potevano raggiungere addirittura un diametro fino a 4 m (13 piedi)[50]. Queste monete venivano ricavate da una pietra calcarea, la particolarità era il deposito di calcite o carbonato di calce cristallizzato che, infiltrandosi nei crepacci, formava delle venature, da cui impossibilità di contraffazione.

Orbene, ciò che veramente caratterizzava questa moneta, tuttavia, risiedeva nel peso, atteso che la pietra Rai poteva arrivare a pesare persino fino a 4 tonnellate. Erano evidenti, ovviamente, da sé le notevoli difficoltà cui si andava incontro ogniqualvolta si presentasse la necessità di spostarla. Proprio perché era sostanzialmente impossibile scambiare materialmente la moneta quando le transazioni avevano luogo in posti lontani tra di loro, si sviluppò un nuovo sistema ben più comodo ed efficiente: era un sistema basato sull'utilizzo dei registri. Ciascun possessore di moneta possedeva, dunque, anche una copia del registro, e quando avveniva una transazione tutti i possessori del registro erano tenuti ad aggiornarlo in ragione del cambio del possessore di quella moneta[51].

Di talché, il rischio di furti o transazioni non consentite era pressoché nullo, non solo perché il Rai sarebbe stato difficile da trasportare e nascondere, ma soprattutto perché tutti conoscevano i diritti su ogni singolo Rai. Infatti, nel sistema economico dell'isola di Yap non si usavano più le pietre fisiche per gli scambi ma il diritto di proprietà sul Rai, che veniva scambiato per beni e servizi. E ciò era possibile poiché ogni scambio tra yapesi veniva annunciato a tutta la comunità che

[50] Cfr. BRYAN M.F., *Island Money*, in *Federal Reserve Bank of Cleveland Research Department*, 2004, pp. 1-4; KOCHERLAKOTA N., *The Technological Role of Fiat Money*, in *Federal Reserve Bank of Minneapolis, Quarterly Review* 22:3, 1998, pp. 2–10.
[51] Cfr. BERENTSEN A., SCHAR F., *A Short Introduction to the World of Cryptocurrencies*, in *Federal Reserve Bank of St. Louis Review*, 100(1), 2018, pp. 1-16.

decideva se "validare" la transazione, quindi tutti gli abitanti erano a conoscenza di tutte le transazioni che avvenivano sull'isola, quello che oggi potremmo definire, come vedremo nel prosieguo della trattazione, un "*distributed ledger*", o "libro mastro distribuito".

Orbene, ciò che maggiormente connotava questo sistema era rappresentato dal fatto che non vi era un'autorità centrale posta a presidio del sistema dei pagamenti: il sistema, invero, era articolato sull'informazione diffusa e distribuita, rappresentata dai registri. Tali registri assicuravano l'unicità della transazione, ossia testimoniavano il fatto che essa, una volta conclusa, non potesse essere soggetta a ripetizione, in quanto l'aggiornamento del registro avrebbe garantito la correttezza e la certezza dei traffici intervenuti. Tutti i possessori, invero, venivano a conoscenza del fatto che quella transazione era già avvenuta una volta. Di talché, i registri contenevano già tutte le informazioni per verificare, *ex-ante*, se il pagamento andrà a buon fine, posto che da essi era possibile risalire alla titolarità della moneta in capo all'acquirente, che si stava impegnando a pagarla in cambio di una certa merce[52]. La sicurezza del sistema, dunque, era rappresentata dal fatto che per effettuare un'operazione illecita nell'isola di Yap bisognava manipolare tutti i registri e convincere tutti gli abitanti della validità di quella determinata transazione; il che avrebbe, ovviamente, richiesto uno sforzo non sostenibile, con la conseguenza che non si rivelava affatto possibile manipolare le transazioni o acquisire proprietà di un oggetto illecitamente.

Si è trattato di un meccanismo che per secoli e in tutte le civiltà le istituzioni bancarie e finanziarie e le pubbliche amministrazioni hanno utilizzato, mediante, appunto, la tenuta dei registri, nei quali veniva posta l'annotazione dei passaggi di proprietà o possesso di un bene o della moneta stessa. In fondo, si tratta di un sistema che trova utilizzo ancora oggi: sebbene con modelli ben più sofisticati e affidabili; invero, questo avviene nello scambio di tantissimi beni, come le case, le automobili, e il denaro tenuto in banca, per i quali esistono registri, tenuti da autorità centrali e collettivamente riconosciute, che si occupano di custodirli e di regolare

[52] Cfr. Cfr. RUBINO DE RITIS, *La moneta digitale complementare: modelli convenzionali di adempimento in criptomonete e prospettive per il sud*, in Aa.Vv., Fintech a cura di Fimmanò e Falcone, Napoli, 2019, pp. 529 ss.; RUBINO DE RITIS M.R., *Virtuale, la quarta generazione di moneta*, in *Rivista del Notariato*, fasc. 6, 2018, p. 1314.

gli accessi agli stessi[53]. Infatti, se tradizionalmente, i registri venivano tenuti su supporto cartaceo, oggi, con la digitalizzazione, molti di essi sono diventati virtuali. Questo ha portato enormi benefici dal punto di vista dell'accessibilità, del costo per la collettività e della sostenibilità.

Orbene, il riferimento ai registri tenuti sull'isola di Yap è utile per comprendere cosa sia la *blockchain*, detta anche di "registro distribuito" – "*Distributed Ledger Technologies*", o "DLTs" –. Solitamente, oggi, si fa risalire la nascita della *blockchain* a *Satoshi Nakamoto*[54], il quale nel 2008 pubblicava *online* un *paper* intitolato "*Bitcoin: A Peer-to-Peer Electronic Cash System*"[55], nel quale veniva chiarito il concetto di *Bitcoin* e si spiegava il funzionamento del sistema di registri che ne tracciavano la circolazione. Un anno più tardi, venivamo emessi primi *bitcoin*, insieme con il *software* destinato a gestirne la circolazione.

Orbene, questa pubblicazione, di sole nove pagine, ha posto le basi e teorizzato il primo sistema, ancora oggi il più diffuso, di pagamento *trustless* basato su tecnologia *blockchain*, unendo una serie di tecnologie già note, ma trovando soluzioni innovative ad alcuni problemi che nascono dalla realizzazione di un meccanismo di pagamento distribuito tra persone distanti con eliminazione di un ente centrale a garantire la certezza dei pagamenti stessi.

In realtà, tuttavia, l'idea di uno strumento di pagamento virtuale risale al 1994, e quindi ben più di dieci anni prima del *paper* di *Sakamoto*, anno, cioè, in cui viene creato *DigiCash*, servizio realizzato da *David Chaum*, in cui però era ancora necessario prevedere l'esistenza di un ente centrale con le funzioni di "stanza di compensazione" delle varie transazioni[56].

L'idea di assicurare l'anonimato delle transazioni all'interno delle reti telematiche deriva dal movimento *cypherpunks*, ossia da un gruppo di soggetti – inizialmente costituito da *Eric Hughes*, *Tim May* e *John Gilmore* – che crearono

---

[53] Sul punto cfr. KEYNES J.M., *Treatise On Money*, Vol. II, 1930, p. 292. In questa sua opera, in particolare, l'Autore riteneva che il trasferimento della proprietà di una moneta Rai rappresentasse "il più antico esempio di '*earmarking*'", ossia l'"attribuzione di una risorsa economica", mettendone in evidenza l'analogia con quanto accadeva per l'oro nei forzieri delle banche centrali.

[54] In realtà non è chiaro se si tratti del vero nome dell'inventore, di uno pseudonimo o addirittura del nome di un gruppo di persone che hanno collaborato al progetto.

[55] Reperibile su *https://bitcoin.org/bitcoin.pdf*.

[56] Cfr. SARZANA F., *La Blockchain*, in Ippolito S., Nicotra M., *Diritto della Blockchain, intelligenza artificiale e IoT*, Milano, 2018, pp. 10 ss.

una *mailing list* sulla quale venivano discussi i temi della *privacy* e della cifratura dei dati[57]. Nel 1993 viene pubblicato il "*Cypherpunk Manifesto*"[58]. Successivamente, nel 1997, viene proposto *Hashcash* da *Adam Back*, un sistema per evitare il fenomeno dello *spam* nella posta elettronica, rendendo oneroso inviare messaggi non desiderati tramite computer, mentre nel 1998 *Wei Dai* pubblicava la sua proposta di *B-money*[59] con cui descriveva per la prima volta un sistema decentralizzato di pagamento, garantito dalla cifratura e dalla c.d. "*proof of stake*", ossia dall'incentivo dei partecipanti ad agire onestamente nel *network* potendo altrimenti perdere i fondi depositati in caso di validazione di transazioni fraudolente. Negli stessi anni *Nick Szabo* propone la definizione di *smart contract*, vale a dire contratti intelligenti capaci di eseguire automaticamente delle transazioni.

Nel 2004, *Hal Finney*, basandosi sui principi di *Hashcash*, teorizza la *proof of work* e nel 2005 *Nick Szabo* pubblica una proposta avente ad oggetto il *Bitgold*, con alla base l'idea sviluppata dallo stesso *Finney*, ma senza porre un limite all'ammontare totale dei *Bitgold* prodotti, conferendo loro un valore diverso a seconda delle capacità computazionali investite per produrli.

Sono queste, in sintesi, le basi che conducono, nel 2008, alla pubblicazione del *paper* di *Satoshi Nakamoto* in cui viene descritto il funzionamento di *Bitcoin*, che porta, il 3 gennaio 2009, alla creazione del "*Genesis Block*" ossia del blocco iniziale della *Blockchain Bitcoin*.

[57] Il movimento "*cypherpunk*" aveva quale principale scopo quello di contrastare le possibili restrizioni delle libertà e del diritto alla *privacy*, derivanti dalla sempre più pervasiva diffusione delle tecnologie informatiche, le quali avrebbero consentito ai governi ed alle grandi società di monitorare e controllare le informazioni sugli individui potendo inferire i loro stili di vita dall'associazione dei dati raccolti nelle transazioni di consumo. Lo strumento principale di contrasto a tale pericolo era stato individuato in una moneta elettronica anonima ed altri strumenti di pagamento non tracciabili, il tutto utilizzando tecnologie crittografiche su larga scala, che avrebbero anche permesso di realizzare sistemi di messaggistica sicuri, contratti digitali e sistemi di identità digitale rispettosi della *privacy*.

[58] Reperibile su *https://www.activism.net/cypherpunk/manifesto.html*.

[59] Reperibile su *http://www.weidai.com/bmoney.txt*.

2.2. La *blockchain*: cos'è e come funziona.

La *blockchain*, oltre ad essere una tecnologia, è anche un'innovazione, un modo di interpretare il grande tema della decentralizzazione e della partecipazione[60], costituendo un processo in cui un insieme di soggetti condivide risorse informatiche per rendere disponibile alla comunità di utenti un *database* virtuale[61].

Essa, infatti, altro non è se non un registro che riporta, in tempo reale, alcune informazioni specifiche che riguardano gli operatori attivi sul mercato. In particolare, il *Financial Times*, nel 2016, l'ha definita come "un *network* di *computer*, che devono unanimemente approvare una transazione affinché questa sia registrata su un registro pubblico, che tutti quelli che appartengono al *network* possono consultare"[62]. Invero, la *blockchain* è una particolare forma di libro mastro distribuito (*distributed ledger*), raffigurabile attraverso l'immagine di una catena in continuo accrescimento, formata da anelli digitali (*block*) all'interno di ciascuno dei quali è racchiuso un certo numero di transazioni[63].

La legge dell'11 febbraio 2019, n. 12[64], all'art. 8 *ter*, rubricato "Tecnologie basate su registri distribuiti e *smart contract*" definisce la *blockchain* come "le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da critto-grafia verificabili da ciascun partecipante, non alterabili e non modificabili".

Nella sostanza, qualsiasi bene virtuale o tangibile, ma rappresentato digitalmente, può essere trasferito mediante la *blockchain* e registrato

---

[60] Cfr. MATTIUZZO F., VERONA N., *Blockchain e smart contract: nuove prospettive per il rapporto di lavoro*, in *Lavoro nella Giurisprudenza*, 2019, fasc. 3, p. 236.
[61] Cfr. MORO VISCONTI R., *La valutazione delle blockchain: internet of value, network digitali e smart transaction*, in *Diritto Industriale*, 2019, fasc. 3, p. 301.
[62] Testualmente, riportava il *Financial Times*: "*a network of computers, all of which must approve a transaction has taken place before it is recorded, in a `chain' of computer code. The details of the transfer are recorded on a public ledger that anyone on the network can see*".
[63] Cfr. RINALDI G., *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 257.
[64] Legge dell'11 febbraio 2019, n. 12, rubricata "Conversione in legge, con modificazioni, del decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione", pubblicata nella Gazzetta Ufficiale del 12 febbraio 2019, n. 36.

definitivamente su ogni blocco di nodi che partecipano alla catena, sulla quale resta traccia di ogni vicenda anche successiva che lo riguardi. Analogamente, la *blockchain* è mezzo di scambio di *bitcoin*, appunto, la moneta digitale decentralizzata e gestita dalla rete dei partecipanti[65].

Nel momento in cui viene attivata una transazione, il sistema ideato è in grado di accertare che tutte le condizioni perché essa avvenga siano correttamente verificate. Solo in quel caso, la transazione ha luogo e il nuovo passaggio/blocco (di criptovaluta, ad esempio) è iscritto nel registro, aggiungendosi a tutti i passaggi precedenti. La *blockchain*, cioè, viene ad arricchirsi di un nuovo blocco; la modifica avviene contemporaneamente in tutti i registri, e perciò tutti i nodi simultaneamente entrano in possesso della nuova informazione che si è aggiunta alla "storia" che già conoscevano.

Dal punto di vista strutturale, la *blockchain* si basa su un *software* libero (*open*) che proprio perché libero è destinato alla democratizzazione della conoscenza e della custodia dei dati, risultato che non sarebbe possibile ove si utilizzasse un software proprietario[66]. Esso si articola in "pagine", appunto i blocchi, concatenate, su ciascuna delle quali è inciso un numero di transazioni, attribuite, in modo indelebile e immutabile ai rispettivi autori attraverso un meccanismo di crittografia a chiave asimmetrica e una marcatura temporale (*timestamping*) che conferisce data certa[67]. Ogni blocco è, dunque, un elenco di transazioni, che costituiscono i dati identificativi dei valori di scambio.

Il punto di forza della *blockchain*, perciò, è che essa non solo registra l'esistenza della transazione, ma ne certifica anche altri elementi informativi, stabilendo in modo inequivocabile le tempistiche in cui la stessa ha avuto luogo[68].

Orbene, questo meccanismo funziona mediante il ricorso alle tecnologie informatiche di tipo digitale e condiviso: invero, la potenza di calcolo unitamente alla connessione *Internet* consente di aggiornare tutti i registri identici esistenti in rete, in tempo reale, cosicché la modifica di un registro comporta l'immediata

---

[65] Cfr. SALITO G., voce *Smart Contracts*, in *Digesto italiano, discipline privatistiche, sezione civile*, Torino, 2019, pp. 393-400.
[66] Cfr. SARZANA F., *La Blockchain*, cit., p. 5.
[67] Cfr. SALITO G., voce *Smart Contracts*, cit., pp. 393-400; PAROLA L., MERATI P., GAVOTTI G., *Blockchain e smart contract: questioni giuridiche aperte*, cit., pp. 681 ss.
[68] Cfr. DI PAOLA N., *Blockchain e Supply chain management*, cit., pp. 70 ss.

sincronizzazione di tutti gli altri registri presenti sulla rete. Quando un *computer* si unisce alla *blockchain*, immediatamente scarica un esemplare del registro, e da quel momento può contribuire a verificare e validare le transazioni. In questo senso, una *blockchain* in cui ogni partecipante può validare le transazioni è detta *permissionless* – nel senso che chiunque può prendere parte al *network* in qualità di nodo e contribuire al suo funzionamento – per distinguerla da quella di tipo *permissioned*, in cui solo i soggetti abilitati possono validare le transazioni[69].

I *computer* della rete vengono detti "nodi" ("*miner*"); i nodi sono tanti quanti sono i computer di coloro che fanno parte della rete e ciascuno di essi diventa uno dei computer (*client*) che partecipa alla validazione delle transazioni e alla loro trasmissione ad altri nodi[70]. Essi aderiscono alla *blockchain* volontariamente e da quel momento ne entrano a far parte in modo integrante, attraverso un contributo in potenza di calcolo, di una rete *peer-to-peer*, la quale consente la condivisione di *file* e si differenzia dai sistemi *server* / *client*, nei quali l'informazione richiesta può essere reperita su un unico *server*, come accade nel caso di una banca dati consultabile *on line*; nel primo caso, invece, l'informazione può essere reperita attingendo a numerosi *client* connessi in modo paritario in quanto non esiste un unico *server*.

L'idea di fondo, è che la *blockchain* sia una infrastruttura condivisa e aperta, nella quale non esistono soggetti coordinatori o regolatori, in grado di regolare o limitare gli accessi ad essa. In sostanza, essa è un registro di transazioni e documenti "dislocato in differenti luoghi e presso differenti soggetti, e nel contempo privo di un'autorità centrale che mantenga il controllo" su di esso[71]. In quanto piattaforma senza intermediari e per ciò stesso decentralizzata, la *blockchain* si contrappone alla tradizionale logica della gestione centralizzata dei dati, caratterizzata dalla presenza di una sola autorità di controllo, come accade quando si ha a che fare con l'utilizzo

[69] Cfr. PISA M., JUDEN M., *Blockchain and Economic Development: Hype vs. Reality*, in *Center for Global Development Policy Paper*, 2017, p. 107; WALPORT M., *Distributed ledger technology: Beyond blockchain*, in *UK Government Office for Science*, 2016, pp. 123 ss.
[70] Cfr. MATTIUZZO F., VERONA N., *Blockchain e smart contract: nuove prospettive per il rapporto di lavoro*, cit., pp. 236 ss.; GAMBINO A.M., BOMPREZZI C., *Blockchain e protezione dei dati personali*, in *Diritto informatico e dell'informatica*, 2019, pp. 619 ss.
[71] Cfr. MANENTE M., *L. 12/2019 - Smart Contract e tecnologie basate su registri distribuiti. Prime note, Studio 1_2019*, in *Consiglio Nazionale del Notariato*, 2019, pp. 1 ss.

dei dati finanziari, per i quali è rimesso alle banche o agli istituti finanziari intervenire per la loro elaborazione.

Anche la *blockchain* è basata su complessi sistemi di codifica e crittografia. Più specificamente, essa si basa sull'*hashing*, come già avviene per i meccanismi delle *password*, diffusamente utilizzato per accedere a numerosi servizi *online*. Le transazioni vengono convalidate da un algoritmo di consenso e crittografate tramite la funzione di "*hash*", che fornisce una sorta di impronta digitale e rende non invertibile l'operazione e rappresenta, sostanzialmente, l'anello di collegamento con il blocco precedente[72].

L'*hash*, in particolare, è una stringa generata sulla base di un algoritmo che funziona solo in un senso. Più specificamente, se un testo è inserito come *input* dell'algoritmo, questo lo trasforma in una sequenza complessa di lettere e numeri che sono associati in modo univoco alla parola iniziale. In altre parole, se la stessa parola fosse immessa nuovamente nell'algoritmo, darebbe origine alla stessa identica stringa di numeri e lettere. Tuttavia, se, invece, partendo dalla stringa complessa di numeri e lettere si volesse risalire alla parola di partenza, questo risulterebbe impossibile. Tale stringa complessa, in questo senso, rappresenterebbe una sequenza di numeri e lettere senza senso. Il blocco, ossia, come detto, l'insieme delle transazioni, viene calcolato basandosi sul codice del blocco digitale precedente e incatenato allo stesso tramite l'operazione di *hash*; ciò permette di creare la catena e di legare un blocco all'altro. La *blockchain* diviene così un *data base* distribuito ed è per questo che si parla di "*Decentralized Ledger Technology*" (DLT).

La *blockchain* aggiunge ulteriori elementi di sicurezza al meccanismo appena descritto. Essa, infatti, presuppone che tutti gli operatori attivi siano in possesso di un esemplare del registro. Le informazioni contenute nel registro non possono essere copiate, ma le modifiche sono eseguite in modo coordinato, benché autonomo, su ciascun registro, attraverso l'esecuzione di codice. I blocchi di operazioni sono, infatti, validati ed eseguiti in modo serrato in maniera tale da non potere più essere modificati dopo un determinato e breve lasso di tempo, dai singoli

[72] Cfr. MORO VISCONTI R., *La valutazione delle blockchain: internet of value, network digitali e smart transaction*, cit., p. 301.

utenti. Perciò, se in un certo nodo dovesse esserci un tentativo di forzatura, ossia di ingresso di un soggetto non abilitato, che inserisce informazioni illegittime, tale tentativo sarebbe immediatamente riconosciuto dagli altri nodi della rete, poiché le informazioni immesse sarebbero difformi da quelle contenute su tutte le altre copie del registro. L'incoerenza delle informazioni su un nodo rispetto a quelle possedute dagli altri, in altre parole, sarebbe un immediato segnale di allarme, che il sistema è in grado di riconoscere. Perciò, per modificare in modo fraudolento il contenuto della *blockchain* non basterebbe un attacco al singolo nodo (come, invece, accade per i registri tenuti da un soggetto unico), ma sarebbe necessario attaccare contemporaneamente tutti i nodi della rete.

Inoltre, il sistema di autenticazione della *blockchain* supera quello classico basato su *username* e *password*, e si basa invece su un sistema di *encryption*. In altre parole, la decentralizzazione delle informazioni e la tecnologia utilizzata aumenterebbe la sicurezza complessiva del sistema e il suo livello di *accountability* riducendo il rischio di errori dovuti a malfunzionamenti o anche ad azioni illegittime[73].

2.3. Le caratteristiche della *blockchain*.

In termini riassuntivi, dunque, la *blockchain* può essere descritta come un database distribuito – ed, infatti, rientra nella più ampia categoria delle *Distributed Ledger Techonology* (DLT) – che consente al medesimo tempo di eliminare la presenza di una terza parte fidata, ossia di un soggetto che svolge le funzioni di validatore delle transazioni, instaurando un meccanismo alternativo di fiducia[74] e di introdurre il concetto di scarsità digitale[75].

---

[73] Cfr. DI PAOLA N., *Blockchain e Supply chain management*, cit., pp. 70 ss.

[74] Cfr. TAPSCOTT D., TAPSCOTT A., *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, 2016, Portfolio, p. 8, il quale lo definisce "*The trust Protocol*".

[75] Cfr. sul punto cfr. PALLADINO A., *L'equilibrio perduto della blockchain tra platform revolution e GDPR compliance*, in *Rivista di diritto dei media*, 2019, pp. 152 ss., il quale scrive: "La *blockchain*, *species* del *genus* delle *distributed ledger technologies*, si configura come una «catena di blocchi», dal momento che i dati, inseriti per mezzo di crittografia asimmetrica, sono allocati in blocchi, accompagnati da *hash* e validazione temporale, tra loro concatenati attraverso il richiamo dell'*hash* del blocco precedente in quello successivo: da questo aspetto deriva la caratteristica dell'immutabilità unilaterale".

E, proprio il concetto di "scarsità digitale" è ciò che rende possibile la creazione di valore, rendendo gli *asset* registrati sulla *blockchain* scambiabili e suscettibili di una valutazione economica. Occorre, infatti, considerare, che, in ambito informatico, ogni insieme di informazioni può essere facilmente replicata, senza costi od oneri aggiuntivi; invero, un qualsiasi *file* può essere facilmente copiato, diffuso e trasmesso, così come qualsiasi informazione registrata su supporto informatico. Il meccanismo della *blockchain* consente, al contrario, di rendere "scarsa" l'informazione, dando quindi valore ad un bene (immateriale) che altrimenti non ne avrebbe. Ciò è possibile tramite l'uso delle tecnologie crittografiche, la cui applicazione ad un determinato *set* di dati rende univocamente identificabili gli stessi, consentendo la loro identificazione e tracciabilità in un sistema che, altrimenti, vede indistinguibili gli originali dalle copie[76].

Oltre a questa, la tecnologia *blockchain* si connota per il possesso di altre peculiarità che la rendono differente rispetto alle altre tecnologie oggi maggiormente usate e che la caratterizzano in maniera specifica ma che, al contempo, ne costituiscono anche il limite[77].

A differenza della maggior parte dei servizi *online*, la *blockchain* è, come detto, decentralizzata. Il problema alla base che si pone è, dunque, quello di assicurare, in assenza di un ente gerarchicamente sovraordinato agli utilizzatori, avente il compito di sorvegliare le operazioni attraverso il mantenimento di una banca dati di riferimento, un meccanismo che sia in grado di conferire al sistema un elevato livello di sicurezza, scongiurando le conseguenze negative di comportamenti fraudolenti o comunque lesivi. Detta problematica, nella *blockchain*, tuttavia, come abbiamo visto, viene superata da un efficiente sistema di sicurezza[78]. Infatti, la *blockchain* è un registro immodificabile, nel senso che le informazioni sono memorizzate in una modalità tale che non è possibile per il

[76] Tuttavia, vi è da rilevare che comunque la legislazione italiana ha già da tempo introdotto il concetto di unicità del documento informatico. Il Decreto Legislativo n. 82/2005 (CAD) distingue tra "duplicato informatico" e "copia informatica", ossia tra un *file* contenente la "medesima sequenza di valori binari del documento originario" ed un *file* che, invece, ha una "diversa sequenza di valori binari". Con la *blockchain*, una volta creata la sequenza di *bit*, ossia l'informazione originaria, tramite l'applicazione della chiave privata e la registrazione del relativo *hash* in un blocco, detta sequenza diviene tracciabile e, quindi, non duplicabile acquisendo unicità all'interno del *network*.

[77] Cfr. sul punto DE FILIPPI P., WRIGHT A., *Blockchain and the law*, *The Rule of Code*, Harvard University Press, 2018, p. 34.

[78] Cfr. RINALDI G., *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 257.

singolo partecipante cancellarle o variarle. I dati registrati, inoltre, in conseguenza dell'utilizzo della crittografia a chiave pubblica, sono non ripudiabili da coloro che li hanno generati, e possono essere sempre verificati. Il sistema, infatti, conserva i *metadati* e le informazioni di contesto delle singole transazioni, rendendo riconducibili le stesse agli account partecipanti al network[79].

Essa ha, inoltre, una vocazione transnazionale che si contrappone alla situazione attuale, in cui le interazioni *online* sono caratterizzate dall'essere veicolate da enti o soggetti i quali operano come detentori delle informazioni – sia che si tratti di effettuare ricerche *online*, di acquistare beni o servizi o di effettuare dei pagamenti –. La gran parte dei servizi prevedono la presenza di un soggetto che opera quale erogatore degli stessi o che intermedia tra altre parti. La *blockchain* consente, invece, di eliminare tale presenza, mettendo in diretto collegamento gli utenti, tramite il meccanismo *peer-to-peer*, in cui ciascuno svolge un ruolo contemporaneamente attivo per la creazione e validazione delle transazioni e passivo per la conservazione della memoria delle stesse. Il *database* delle informazioni è distribuito su tutti i nodi del *network*, e ciò conferisce anche la caratteristica di transnazionalità della tecnologia. Qualora un Paese decida di bloccare l'accesso al *network* comunque tutte le transazioni sarebbero conservate in ciascuno dei nodi, potendo così facilmente ripristinarne l'operatività dello stesso.

Altra caratteristica peculiare della *blockchain* è il meccanismo di incentivazione dei partecipanti. La tecnologia è logicamente strutturata per indurre ad agire in buona fede, incentivando la partecipazione al sistema, tramite meccanismi di guadagno e rendendo estremamente difficili le condotte abusive. Su tali incentivi si riflettono anche meccanismi di mercato, a volte speculativi, in cui entrano in gioco i valori assunti dalle criptovalute in un dato momento rispetto ai costi necessari a produrle.

Ancora, la tecnologia *blockchain* si connota per consentire la "pseudonimizzazione" dei suoi partecipanti dato che, almeno su *Bitcoin*, i titolari degli *account* non sono direttamente identificabili. Infatti la *blockchain* non include

[79] Cfr. SARZANA F., *La Blockchain*, cit., p. 19.

informazioni che consentono di risalire (direttamente) alla persona che ha effettuato il trasferimento, ma soltanto alla sua chiave pubblica[80].

Tuttavia, non si è esitato ad evidenziare che un tale mascheramento non esclude la possibilità di ricavare, attraverso un incrocio dei dati contenuti nella *blockchain* unitamente alle tracce lasciate sul *web* dal soggetto che ha concretamente disposto le operazioni, la reale identità dell'individuo cui è riconducibile la chiave pubblica e, quindi, tutte le transazioni che lo hanno riguardato[81]. Ecco perché si è ben presto posta la questione relativa alla tensione fondamentale che in *blockchain* può venirsi a creare tra le esigenze postulate dalla tracciabilità delle operazioni e la riservatezza dei suoi utilizzatori. Come si è detto, infatti, il funzionamento del sistema è reso possibile dall'esistenza di un registro pubblico, perpetuo e immodificabile, contenente tutte le transazioni avvenute. È evidente che questo limite – come vedremo più approfonditamente nel prosieguo della trattazione – costituisce un *vulnus* certamente non trascurabile nei confronti della tutela della *privacy*, visto il carattere personale e la rilevanza delle informazioni che possono essere contenute all'interno della *blockchain*, soprattutto nel caso in cui tali dati non si riferiscano soltanto a trasferimenti di fondi.

Ulteriori caratteristiche della tecnologia *blockchain* sono, infine, la capacità di creare meccanismi per la formazione del consenso nell'ambito del *network* senza la necessità di un organismo centralizzato[82]; la possibilità di creare *software* che operano quali agenti autonomi, distribuiti su tutto il *network*, che agiscono in maniera indipendente e che possono svolgere funzioni in maniera automatica al verificarsi di alcune condizioni, senza dover dipendere da un singolo soggetto erogatore.

---

[80] Cfr. FRANCO P., *Understanding Bitcoin. Cryptoghraphy, Enginnering and Economics*, Padstow, 2014, pp. 209 ss.

[81] Cfr. EENMAA-DIMITRIEVA H., SCHMIDT-KESSEN M.J., *Regulation Through Code as a safeguard for implementing smart contracts in no-trust environments*, in *European University Institute Working Papers*, 2017, fasc. 13, pp. 17-19.

[82] Sul punto più specificamente v. FINOCCHIARO G., *Il contratto nell'era dell'intelligenza artificiale*, cit, pp. 456 ss.

2.4. (*Segue*) Le tipologie di *blockchain*: pubbliche, ibride e private.

Nell'ambito delle varie tipologie di *blockchain* esistono alcune distinzioni in base alla possibilità di accesso ed al grado di distribuzione delle stesse. Semplificando, si possono individuare tre grandi tipologie di *blockchain*[83], sulla base di alcune caratteristiche comuni. Le varianti della *blockchain* possono essere suddivise in pubbliche (*permissionless*), pubbliche-private o ibride e private (*permissioned*). Non si tratta, a ben vedere, di una classificazione rigida in quanto gli elementi caratterizzanti queste diverse declinazioni potrebbero essere tra loro combinanti in infinite varianti al fine di meglio adattarsi alle specifiche applicazioni.

Anzitutto, vi sono le c.d. *blockchain* pubbliche (c.d. *permissionless*) – realizzate con *software open source* –, le quali si connotano per essere liberamente accessibili a chiunque, in quanto non sono previste restrizioni circa la lettura delle transazioni, l'effettuazione delle stesse e la possibilità di partecipare al meccanismo di consenso. Si tratta della tipologia più "pura" della *blockchain* caratterizzata da strutture completamente e totalmente distribuite. Nessun utente della rete ha privilegi sugli altri, nessuno può controllare le informazioni che vengono memorizzate su di essa, modificarle o eliminarle, e nessuno può alterare il protocollo che determina il funzionamento di questa tecnologia.

Le *blockchain* pubbliche hanno tendenzialmente una vocazione globale, creano dei meccanismi di fiducia tra i partecipanti, non prevedono barriere all'ingresso nel *network* e tendenzialmente sono sempre accessibili[84]. Nonostante i dati registrati su queste *blockchain* siano pubblici, questi vengono crittografati per mantenere un sufficiente livello di *privacy*. Si utilizzano, a tal fine, dei codici alfanumerici corrispondenti a chiavi di cifratura e, a meno che non vengano ricondotti all'identità della persona del mondo reale che ne è il proprietario, di fatto rendono non conoscibile l'identità del titolare[85].

---

[83] La classificazione è stata tipizzata dall'Osservatorio *blockchain & distributed ledger* della *School of Management* del Politecnico di Milano.
[84] Cfr. BELLINI M., *Blockchain & Bitcoin*, 2018, Milano Finanza, pp. 41 ss.
[85] Cfr. ARCELLA G., MANENTE M., *Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza*, in *Notariato*, 2020, fasc. 1, p. 23.

Nelle *blockchain* ibride, invece, il meccanismo di consenso sulle transazioni è controllato da un insieme di nodi preselezionati, i quali hanno un'influenza maggiore rispetto agli altri ed anzi, tramite varie soluzioni (solitamente di voto), determinano quali transazioni possono essere incluse nei blocchi. In questo caso, la *blockchain* può essere accessibile al pubblico o limitata ai partecipanti. Sono *blockchain* parzialmente decentrate, in cui i nodi vengono chiamati "*contributors*" e non sono posti sullo stesso piano rispetto alle operazioni che possono compiere nel sistema. Le *blockchain* ibride si prestano a casi d'uso in cui è necessario mantenere il governo sulla registrazione delle transazioni, ma è possibile, e desiderabile, rendere pubblica la consultazione della *blockchain*[86].

Infine, le *blockchain permissioned* sono soggette ad un'autorità centrale che determina chi possa accedervi. Oltre a definire chi è autorizzato a far parte della rete, tale autorità può anche definire quali siano i ruoli che ciascun utente può ricoprire all'interno dell'ambiente, definendo anche regole sulla visibilità dei dati registrati. Esse introducono, quindi, il concetto di *governance* e centralizzazione in una rete che nasce come assolutamente decentralizzata e distribuita[87].

Una *blockchain* privata presenta una serie di vantaggi rispetto quella pubblica, quali la possibilità di modificare le regole della *blockchain*, ripristinare le transazioni, modificare i saldi, ecc. Si presta ad essere utilizzata per applicazioni ed utilizzi sia da parte di privati ed aziende, che possono impiegarla per gestire transazioni ricorrenti tra loro, sia in alcuni ambiti della Pubblica Amministrazione in cui è necessario mantenere un governo delle transazioni che vengono registrate ed il controllo formale e di legittimità da parte dell'Autorità amministrativa.

In generale sono quattro gli elementi distintivi delle *blockchain* private. In primo luogo l'"infrastruttura", in quanto le *blockchain* private devono essere

[86] Si pensi, ad esempio, a tutti i registri pubblici distribuiti, in cui più Amministrazione pubbliche partecipano nell'inserire (o validare) informazioni che per loro natura sono però destinate alla pubblicità. Si potrebbe ipotizzare l'adozione di una tale tecnologia nell'ambito dei procedimenti amministrativi a cui partecipano diverse Pubbliche Amministrazioni, ad esempio tramite conferenza di servizi, in cui ognuna di esse ha un ruolo ed una potestà amministrativa autonomi. La validazione delle informazioni, tramite il meccanismo del "voto dei pochi" permetterebbe di registrare su una *blockchain* ibrida gli esiti delle singole valutazioni delle Pubbliche Amministrazioni. La pubblicità delle informazioni garantirebbe d'altra parte la trasparenza dell'agire amministrativo, senza possibilità di modificare ex post le varie fasi della procedura.

[87] Cfr. ARCELLA G., MANENTE M., *Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza*, cit., p. 23.

attestate su reti a loro volta private, la cui sicurezza è gestita dai partecipanti alla *blockchain* in modo da poter così garantire il meccanismo di fiducia. Ed infatti, proprio perché una *blockchain* privata non può contare sulla sua diffusione, che costituisce la caratteristica di quelle pubbliche e ne assicura l'immodificabilità delle transazioni tramite un meccanismo distribuito di consenso difficilmente aggredibile, diventano essenziali gli aspetti di sicurezza dell'infrastruttura, che non deve consentire a soggetti estranei al *network* di parteciparvi, pena il venir meno dell'affidabilità di quanto registrato sulla *blockchain*.

In secondo luogo, l'"ecosistema". Per ecosistema si intende la necessità che i partecipanti ad una *blockchain* privata condividano, per quanto attiene alla partecipazione al *network*, gli stessi valori, obiettivi e regole. L'efficacia di una *blockchain* privata poggia, infatti, sulla fiducia reciproca dei partecipanti e sull'aspettativa che ciascuno di essi ha nel fatto che gli altri agiranno coerentemente con gli obiettivi del *network*.

In terzo luogo le "applicazioni". La componente applicativa delle *blockchain* private deve seguire le logiche tecnologiche e di *governance* che sono definite dagli attori del *network*. In una *blockchain* le regole di partecipazione vengono, per così dire, direttamente definite a livello di *software* e pertanto gli sviluppatori devono agire in stretta collaborazione con i soggetti che intendono partecipare alla *blockchain* privata.

Infine, la "*governance*", la quale costituisce l'insieme di regole condivise da tutti gli attori, definite sulla base degli obiettivi del progetto e dei risultati attesi. Tramite la possibilità di modulare i meccanismi di consenso e di creare *smart contract* che eseguono in maniera automatica determinate operazioni, la *governance* può essere direttamente disciplinata nel codice *software* che assume così una funzione "regolatoria".

2.5. (*Segue*) La formazione del consenso nell'ambito della *blockchain*.

Nella disamina sul funzionamento e sulle caratteristiche della *blockchain* è senz'altro necessario considerare un aspetto importante, ossia la formazione del consenso all'interno del *network*, quale elemento peculiare della tecnologia in

commento. Si tratta di un aspetto meritevole di considerazione in quanto in un sistema decentralizzato come quello poc'anzi descritto, la gestione corretta del consenso è ciò che consente la necessità della presenza di un soggetto che svolga le funzioni di validazione delle operazioni che vengono svolte dagli attori del *network*.

Il pregio maggiore del sistema che stiamo analizzando, infatti, è quello di permettere a individui estranei tra loro di poter confidare nella sicurezza delle transazioni immesse nella *blockchain*, senza dover riporre fiducia in soggetti intermediari, enti certificatori, oppure nel potere deterrente o coercitivo dell'ordinamento giuridico[88].

Ciò spiega perché il protocollo del "consenso distribuito" viene ad assumere un ruolo centrale non solo per determinare gli equilibri del sistema, ma anche per rispondere alle esigenze che lo stesso si propone di soddisfare, in modo che, a seconda degli obiettivi che si vogliono raggiungere con l'utilizzo della *blockchain*, sarà necessario optare per il meccanismo di formazione del consenso più adeguato al raggiungimento degli stessi[89].

D'altro canto, sulla solidità ed efficacia del metodo di formazione del consenso poggiano le aspettative di fiducia nelle transazioni registrate sulla *blockchain*. Ciò comporta una possibile responsabilità degli sviluppatori e di coloro che hanno realizzato le varie tecniche di validazione del consenso nei confronti degli utilizzatori del sistema. Il problema alla base è quello di assicurare, in assenza di un ente gerarchicamente sovraordinato agli utilizzatori, avente il compito di sorvegliare le operazioni attraverso il mantenimento di una banca dati di riferimento, un meccanismo che sia in grado di conferire al sistema un elevato livello di sicurezza, scongiurando le conseguenze negative di comportamenti fraudolenti o comunque lesivi.

Detta problematica, viene superata – ma non risolta in termini assoluti – mediante un approccio di tipo probabilistico, fondato sull'impiego della teoria dei giochi, che si concretizza in un ingegnoso algoritmo di consenso distribuito, la cui struttura si basa su un sistema di incentivazione economica che induce i partecipanti

[88] Cfr. WERBACH K., CORNELL N., *Contracts Ex Machina*, in *Duke Law Journal*, 2017, p. 67, consultabile su *https://papers.ssrn.com.*
[89] Cfr. GARAVAGLIA R., *Tutto su blockchain*, Milano, 2018, p. 59.

a rispettare le regole di funzionamento del protocollo, rendendo tendenzialmente svantaggiose le condotte disoneste[90].

In particolare, esistono varie soluzioni tecniche, basate su algoritmi conosciuti, per creare i meccanismi di consenso. In particolare, la prima vera soluzione informatica al problema del "consenso distribuito" si a *Satoshi Nakamoto*, il quale nell'ideare il complesso apparato tecnologico alla base del funzionamento dei *bitcoin* ha inventato un meccanismo informatico noto come "*Proof of Work*", che consiste in un complesso (quanto ingegnoso) meccanismo di competizione matematica tra i computer volto a consentire a nodi di una rete (che non si conoscono tra loro) di raggiungere ugualmente il consenso nella validazione delle transazioni. In pratica, i nodi della *blockchain* si sfidano nella soluzione di un problema matematico, talmente difficile da rendere impossibile conoscere in anticipo quale nodo sarà in grado di offrire per primo la soluzione, essendo risolvibile solo procedendo per tentativi. Ma allo stesso tempo, altra caratteristica fondamentale, il meccanismo è tale per cui, una volta individuata la soluzione, essa potrà essere verificata pressoché istantaneamente da tutti i nodi connessi alla rete, in modo tale da poter essere da tutti validata[91].

Gli informatici hanno, tuttavia, sperimentato, nel corso del tempo, nuovi e differenti sistemi di consenso distribuito, soprattutto in quanto la *Proof of Work* si sta rilevando eccessivamente dispendiosa richiedendo ingenti risorse in termini di energia elettrica e di *hardware* necessari al suo funzionamento. Tra queste vi è la "*Proof of Stake*" (PoS), secondo il quale un nodo ha la possibilità di validare delle transazioni sulla base del quantitativo di *asset* che possiede, contemperato, in alcune ipotesi, anche dal periodo di tempo di possesso di dette risorse. Tale meccanismo si fonda sulla presunzione che più *asset* un utente possiede di una *blockchain* (e da più tempo) meno interesse lo stesso può avere nell'attaccare il sistema; o la "*Delegated Proof of Stake*", in cui ciascun nodo che possiede risorse del sistema può delegare un altro nodo a validare la transazione mediante un meccanismo di voto; o, ancora, il *Deposit-based consesus*, tramite il quale i nodi che vogliono

[90] Cfr. SUNGWOOD K., *Game Theory Solutions for the Internet of Things: Emerging Research and Opportunities*, Hershey, 2017, pp. 87 ss.
[91] Cfr. ARCELLA G., MANENTE M., *Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza*, cit., p. 23. In particolare l'Autore scrive: "la *proof of work* dei *bitcoin* si basa su problemi matematici difficili da risolvere, ma al tempo stesso facili da verificare".

partecipare al *network* devono effettuare un deposito vincolato prima di poter proporre un blocco della *blockchain*[92], nonché meccanismi basati sulla reputazione, ossia sistemi in cui viene designato un *leader* (un nodo fidato) sulla base della reputazione che ha acquisito nel *network* con il trascorrere del tempo.

Notevole importanza riveste la "*Proof of Authority*" (PoA) in cui un nodo è autorizzato a validare le transazioni sulla base dell'identità del nodo stesso, posto che la dottrina ha ritenuto che questa tecnica può sembrare più familiare per gli utenti che hanno esperienza con i database in cui solo coloro che sono muniti di specifiche autorizzazioni possono modificare o aggiungere dati. Pertanto, potrebbe essere il meccanismo di gestione del consenso più applicabile per molte applicazioni di *blockchain* nel settore pubblico, in quanto può essere adattato per rappresentare la complessità dei procedimenti di governo dell'Autorità amministrativa e dei relativi processi decisionali[93].

Il meccanismo di formazione del consenso su una rete *blockchain* è, peraltro, connesso alla tipologia di utilizzo a cui essa è destinata ed al grado di apertura del *network*. Invero, in una *blockchain* pubblica ed aperta va da sé che il sistema con cui si crea la fiducia sulle transazioni registrate dai vari nodi assume una particolare importanza, sia in quanto i partecipanti sono tra di loro sconosciuti, sia per evitare attacchi da parte di terzi. In *blockchain* di tipo ibride o chiuse tali esigenze rilevano meno, considerato che i partecipanti – chiamati "*contributors*" – nella maggior parte dei casi sono conosciuti ai gestori del sistema ed in quanto, trattandosi appunto di *network* non facilmente accessibili dall'esterno, la sicurezza deve essere gestita principalmente a livello di reti e strumenti impiegati.

---

[92] A queste possono aggiungersi, la "*Proof of Elapsed Time*", che basa il processo di validazione sul trascorrere del tempo; la "*Proof of importance*", che oltre a verificare il possesso degli *asset* da parte del nodo, esamina anche l'utilizzo e le movimentazioni degli stessi per stabilire un livello di fiducia ed importanza; il "*Federated consensus*" o "*Byzantine consensus*", in cui i nodi propagano solamente le transazioni che sono state già validate dalla maggioranza dei nodi fidati; "*Pratical Byzantine Fault Tolerance*", con cui si raggiunge la replicazione dello stato delle macchine attraverso meccanismi di voto; la "*Proof of Activity*", che combina la *proof of work* e la *proof of stake*; la "*Proof of Capacity*", che richiede che venga dedicato un determinato spazio dei dischi di memoria per consentire la validazione dei blocchi; la "*Proof of Existence*", che si basa sul possesso del nodo di determinati documenti o autorizzazioni; la "*Proof of Presence*", fondata sulla geolocalizzazione del nodo, ed utilizzata soprattutto in ambito IOT; la "*Proof of Storage*", per cui i nodi devono condividere ed allocare dello spazio disco in un *cloud* distribuito. Cfr. sul punto CONTALDO A., CAMPARA F., *Blockchain, criptovalute, smart contract, industria 4.0. Registri digitali, accordi giuridici e nuove tecnologie*, Pisa, 2019, pp. 12 ss.

[93] Cfr. SARZANA F., *La Blockchain*, cit., pp. 22 ss.

Infine, bisogna considerare che il meccanismo di consenso è l'elemento su cui si concentrano gli attacchi alla sicurezza della *blockchain*, dato che la validazione, o la modifica, delle transazioni sono regolate proprio mediante tale procedimento. Così mentre in una *blockchain* pubblica la distribuzione del *network* può rendere più complessa (e soprattutto antieconomica) la possibilità di un attacco, in una *blockchain* privata che utilizzi meccanismi di consenso fondati sull'autorità, identità o capacità dei singoli nodi la sicurezza del *network* è direttamente proporzionale alla sicurezza dei sistemi su cui sono attestati i nodi validatori. In questi casi si potrebbero rinvenire dei profili di responsabilità dei gestori di tali sistemi, qualora non vengano da essi adottati standard elevati di sicurezza per proteggere le macchine e le reti che assumono ruoli rilevanti nella formazione dei meccanismi di consenso della *blockchain* a cui partecipano.

Nel complesso, in definitiva, il sistema realizza una condizione che è stata definita di "*trustless trust*"[94], vale a dire un meccanismo di affidamento collettivo che per sostenersi ed operare non ha bisogno del supporto di organi gerarchicamente sovraordinati rispetto ai suoi utilizzatori: gli eventuali contrasti non vengono risolti attraverso l'intervento di un'autorità sovraordinata, ma automaticamente, nell'approccio strutturalmente decentralizzato del consenso distribuito[95].

3. Profili giuridici: il quadro europeo e italiano di riferimento.

Dopo aver analizzato gli aspetti tecnologici attinenti al funzionamento della *blockchain*, passiamo ora a vedere i profili giuridici, mediante l'analisi dei diversi atti di riferimento europei e nazionali.

Orbene, la prima considerazione da cui partire è che lo sviluppo della tecnologia in esame e il suo uso sempre più diffuso oltre i confini del settore

[94] Cfr. HOFFMAN R., *Why the blockchain matters*, in *Wired*, 15 febbraio 2015.
[95] Cfr. RINALDI G., *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 257.

finanziario e dei *bitcoin* hanno evidenziato il problema della mancanza di un'adeguata normativa sia a livello nazionale sia a livello comunitario. Non vi sono, infatti, fonti del diritto italiano o comunitario, né di primo né di secondo livello, che regolino organicamente tale settore né, allo stato, si può parlare di prassi commerciali diffuse, tali da costituire una *lex mercatoria* a cui gli operatori del mercato possano fare riferimento[96].

Fermo restando, tuttavia, la mancanza di norme aventi ad oggetto la tecnologia *blockchain* e vista la rapida e continua evoluzione della stessa, nonché la relativa diffusione in molteplici settori, le istituzioni e il legislatore hanno, in varie occasioni, iniziato a mostrare sempre più interesse e hanno altresì cominciato ad interrogarsi circa la necessità di intervenire con una normativa uniforme che garantisca un approccio omogeneo ai problemi che scaturiranno da una diffusione sempre maggiore della stessa.

A livello sovranazionale, merita menzione, anzitutto, la Risoluzione del Parlamento europeo del 3 ottobre 2018[97] sulle tecnologie di registro distribuito e *blockchain*, la quale nell'analizzare, appunto, la tecnologia *blockchain* indicandone le possibili applicazioni, le reputa strumenti atti a creare fiducia attraverso la disintermediazione. In particolare, con tale Risoluzione, il Parlamento invita la Commissione, previo ausilio delle pertinenti organizzazioni internazionali operanti nel settore, quali ISO, UIT, CEN-CELENEC, ad attivare le procedure ritenute necessarie per forgiare un sistema normativo particolarmente tecnico, comune ai vari Paesi aderenti all'Unione Europea.

In particolare, secondo quanto disposto dalla Risoluzione in oggetto, le tecnologie di registro distribuito sono tecnologie "in grado di migliorare l'efficienza dei costi delle transazioni eliminando intermediari e costi di intermediazione, oltre ad aumentare la trasparenza delle transazioni, ridisegnando anche le catene del valore e migliorando l'efficienza organizzativa attraverso un decentramento affidabile".

---

[96] Cfr. PAROLA L., MERATI P., GAVOTTI G., *Blockchain e smart contract: questioni giuridiche aperte*, cit., pp. 681 ss.

[97] Cfr. PARLAMENTO EUROPEO, Risoluzione del 3 ottobre 2018 P8_TA-PROV(2018)0373, rubricata "Tecnologie di registro distribuito e *blockchain*: creare fiducia attraverso la disintermediazione".

La Risoluzione, anche se non vincolante, muove dalla considerazione che le tecnologie di registro distribuito (DLT) e *blockchain* possono costituire "uno strumento che rafforza l'autonomia dei cittadini dando loro l'opportunità di controllare i propri dati e decidere quali condividere nel registro, nonché la capacità di scegliere chi possa vedere tali dati" e, grazie ai necessari meccanismi di cifratura e controllo, "può democratizzare i dati e rafforzare la fiducia e la trasparenza, fornendo un percorso sicuro ed efficace per l'esecuzione delle transazioni", posto che la *blockchain* consente una sinergica interazione fra tecnologia, politiche gestionali ed aspetti economici[98].

Tuttavia, il Parlamento europeo, essendo consapevole della presenza di pericoli riscontrabili nell'utilizzo di tali tecnologie, sottolinea, altresì, che i rischi e i problemi non sono ancora completamente noti, chiarendo, altresì, che le *distributed ledger technologies*, quali tecnologie in continua evoluzione, necessitano di "un quadro favorevole all'innovazione che consenta e incoraggi la certezza del diritto e rispetti il principio della neutralità tecnologica, promuovendo nel contempo la protezione dei consumatori, degli investitori e dell'ambiente, aumentando il valore sociale della tecnologia, riducendo il divario digitale e migliorando le competenze digitali dei cittadini".

In sostanza, il merito del Parlamento europeo è stato quello di aver evidenziato le potenzialità e le implicazioni giuridiche derivanti dall'utilizzo della *blockchain*, sottolineando al contempo la necessità che il suo utilizzo risulti, tuttavia, conforme alla normativa europea, soprattutto a quella in materia di protezione dei dati personali.

A livello europeo rileva, altresì, l'istituzione da parte della Commissione europea dell'*EU Blockchain Observatory and Forum* del primo febbraio 2018[99] e dell'*European Blockchain Partnership* del 10 aprile 2018, organismo cui aderiscono, al momento, 27 Paesi europei.

---

[98] Cfr. MATTIUZZO F., VERONA N., *Blockchain e smart contract: nuove prospettive per il rapporto di lavoro*, cit., pp. 236 ss. In particolare, la Risoluzione del Parlamento Europeo ne sottolinea l'importanza strategica per le infrastrutture pubbliche, anche in termini di riduzione del peso burocratico, di potenziamento dell'*eGovernment* e dell'"ulteriore riduzione degli oneri amministrativi a carico di cittadini, imprese e pubbliche amministrazioni".

[99] EU BLOCKCHAIN OBSERVATORY AND FORUM su *eublockchainforum.eu*.

All'*EU Blockchain Observatory and Forum* spetta il compito di raccogliere informazioni, mappare le principali iniziative esistenti, monitorare gli sviluppi e analizzare le tendenze, esaminare il potenziale socio-economico e affrontare le sfide, cercando di garantire un approccio uniforme e comune a livello europeo. Con questo progetto, la Commissione mira ad affrontare le sfide poste dai paradigmi sottesi al *blockchain* (semi-anonimia, tracciabilità, irreversibilità, oltre alla già citata disintermediazione), consolidare le competenze, ampliare le iniziative esistenti, garantire il funzionamento della tecnologia *blockchain* a livello transfrontaliero ed assicurare un approccio uniforme a livello europeo[100].

L'*EU Blockchain Observatory and Forum* ha, a tal fine, istituito due gruppi di lavoro per identificare e ricercare le iniziative esistenti basate su *blockchain*: "*The Blockchain Policy and Framework Conditions Working Group*", deputato a definire le condizioni politiche, legali e regolamentari necessarie per la diffusione su larga scala delle applicazioni basate sulla *blockchain*, e "*The Use Cases and Transition Scenarios Working Group*", chiamato a concentrarsi sui casi di utilizzo più promettenti, con particolare attenzione alle applicazioni del settore pubblico come identità e servizi pubblici, assistenza sanitaria, energia e rendicontazione ambientale[101].

L'*European Blockchain Partnership* ha come obiettivo quello di consolidare il ruolo dell'Europa nello sviluppo e nella diffusione della tecnologia *blockchain*, mediante un approccio di carattere uniforme a livello europeo, che punta ad evitare un approccio frammentato dei vari attori del settore e a consolidare il ruolo dell'Europa nello sviluppo e diffusione della tecnologia *blockchain*. Con una dichiarazione sottoscritta in pari data, ognuno dei Paesi partecipanti si è impegnato a nominare un rappresentante che lavorerà assieme all'esecutivo

---

[100] Cfr. PAROLA L., MERATI P., GAVOTTI G., *Blockchain e smart contract: questioni giuridiche aperte*, cit., pp. 681 ss.

[101] In particolare, rivestono interesse soprattutto i *report* tematici prodotti dall'Osservatorio, che affrontano anche le sfide giuridiche poste da tale tecnologia. Ai fini dell'analisi qui condotta, devono essere considerati il *report* "*Legal and regulatory framework of blockchains and smarts contracts*", pubblicato il 27 settembre 2019, e il *report* "Blockchain and the GDPR", pubblicato il 16 ottobre 2018. Cfr. *https://www.eublockchainforum.eu/eu-blockchain-observatory-forum*. Importante è, altresì, il *report* "*Blockchain for digital government. An assessment of pioneering implementations in public services*" del *Joint Research Centre* (JRC), pubblicato il 23 aprile 2019. Cfr. *https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-digital-government*.

comunitario per stabilire le linee di intervento della *Partnership* e collaborerà con l'Osservatorio e Forum della UE sulla *blockchain*[102].

A tal fine, dunque, ai rappresentanti dei Paesi partecipanti è richiesta collaborazione, al fine di stabilire le linee di intervento utili per sfruttare il potenziale dei servizi basati sulla *blockchain* a beneficio dei cittadini, della società e dell'economia. Tra queste iniziative, merita di essere considerata la cooperazione avviata per la creazione dell'*European Blockchain Services Infrastructure* (EBSI), capace di supportare la fornitura di servizi pubblici transfrontalieri in tutta l'Unione Europea, utilizzando la tecnologia *blockchain* e garantendo alti *standard* di sicurezza e protezione dei dati personali[103].

Infine, merita di essere citato, altresì, il *Focus Group* congiunto sul *blockchain* costituito dalla *European Committee for Standardization* (CEN) e la *European Committee for Electrotechnical Standardization* (CENELEC). L'obiettivo per il quale questo organismo è stato istituito è quello di individuare potenziali profili di standardizzazione e specifiche esigenze di normazione a livello europeo, supportando le iniziative di standardizzazione in fase di sviluppo ad opera della *International Organization for Standardization* col progetto *Iso/TC 307 Blockchain and distributed ledger technologies*. Al *Focus Group*, inoltre, spetterà di affiancare le istituzioni europee nell'analisi e nello sviluppo delle potenzialità insite in questa tecnologia.

A livello nazionale, il segretario generale della Fim-Cisl, Marco Bentivogli, ha lanciato *Blockchain Italia*, il manifesto che intende promuovere l'utilizzo della tecnologia *blockchain* per migliorare i processi dell'industria 4.0[104], nel quale si

---

[102] Cfr. PAROLA L., MERATI P., GAVOTTI G., *Blockchain e smart contract: questioni giuridiche aperte*, cit., p. 681.

[103] Cfr. *https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership* e *https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi*. In particolare, è previsto che l'*European Blockchain Services Infrastructure* (EBSI) si trasformi in una rete di nodi distribuiti in tutta Europa e diventerà un *Building Block del Connecting Europe Facility* (CEF), fornendo *software*, specifiche e servizi riutilizzabili per supportarne l'adozione da parte delle istituzioni dell'Unione Europea e delle Pubbliche Amministrazioni europee.

[104] Cfr. BENTIVOGLI M., CHIRIATTI M., *Così la blockchain aumenta l'umanità del lavoro*, in *Il sole 24 ore Commenti del 12 agosto 2018*, *dossier* Manifesto per un nuovo bene pubblico, in *http://www.ilsole24ore.com/art/notizie/2018-08-11/cosi-blockchain-aumenta-l-umanita-lavoro203658.shtml?uuid=AEBXOWZF*. Bentivogli, in particolare, propone una importante applicazione del sistema *blockchain* alla contrattualistica del lavoro. Egli muove dall'assunto secondo cui nel rapporto sotteso a tale contratto si registra la presenza di diversi *stakeholders*, quali appunto il lavoratore, il datore, gli istituti previdenziali ed assicurativi e financo gli organi ispettivi. Tra questi

afferma che la tecnologia consente di aumentare la sicurezza e la riservatezza delle informazioni, la certezza e la velocità nelle transazioni fra le parti riducendo attriti e costi. Ciò dovrebbe tradursi in incrementi di produttività[105].

Sul piano legislativo, a tal fine, rileva il già citato art. 8 *ter* del decreto legge n. 135 del 2018, convertito in legge n. 12 del 2019, il quale, in particolare, tratta esplicitamente di tali tecnologie, definendo, come abbiamo detto, le tecnologie basate su registri distribuiti e una rilevante applicazione, gli *smart contracts*, conferendo specifici effetti giuridici e demandando la regolazione tecnica a *standard* e linee guida di competenza dell'Agenzia per l'Italia digitale (AgID)[106]. Peraltro, nonostante la tematica riguardi una significativa innovazione tecnologica, il legislatore ha optato per la non integrazione del Decreto Legislativo n. 82 del 2005, ossia il Codice dell'amministrazione digitale (CAD), preferendo, al contrario, lasciare la norma formalmente fuori dal Codice, seppure, per ambito di materia e per i contenuti trattati, potesse ambire a farne parte, in considerazione del fatto che il Decreto Legislativo n. 82 del 2005 dovrebbe porsi quale riferimento principale in tema di innovazione[107].

La definizione data alle *distributed ledger technologies* dalla norma è stata, tuttavia, oggetto di critiche da parte della dottrina per il fatto che rischia di confondere le *distributed ledger technologies* e le *blockchains*, dal momento che alcune caratteristiche evocano più propriamente queste ultime, in particolare nella tipologia *permissionless* (inalterabilità, immodificabilità e verificabilità dei dati da parte di ciascun partecipante), e, di conseguenza, si rischia di determinare una sovrapposizione inappropriata tra i due fenomeni, che in realtà sono differenti: la *blockchain* è una particolare tipologia, una *species* del *genus* delle *distributed ledger technologies*, dotata di proprie caratteristiche distintive[108].

---

attori insistono obblighi di comunicazione, oggi resi meno farraginosi grazie alla sostituzione dell'invio di materiale cartaceo con certificazioni informatiche, non ancora in grado di snellire adeguatamente il cascame burocratico.

[105] Cfr. MATTIUZZO F., VERONA N., *Blockchain e smart contract: nuove prospettive per il rapporto di lavoro*, cit., pp. 236 ss.

[106] Cfr. sul punto, BOMPREZZI C., *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, in *Diritto, mercato e tecnologia*, 2019, pp. 1-7; SARZANA F., *La Blockchain*, cit., pp. 17-23.

[107] Cfr. SARZANA F., *La Blockchain*, cit., p. 18; GAROFALO D., *Blockchain, smart contract e machine learning: alla prova del diritto del lavoro*, in *Lavoro nella Giurisprudenza*, 2019, fasc. 10, p. 869.

[108] Cfr. sul punto, BOMPREZZI C., *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, cit., p. 2; SARZANA F., *La Blockchain*, cit., p. 18.

La disposizione chiarisce che la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'art. 41 del Regolamento (UE) n. 910/2014; ai fini della produzione di tali effetti le tecnologie basate su registri distribuiti devono possedere gli *standard* tecnici individuati dall'AgID[109].

A livello strategico, in Italia nel dicembre 2018 è stato nominato dal Ministero dello Sviluppo Economico un gruppo di esperti, formato da trenta profili multidisciplinari, provenienti da diversi contesti di riferimento, quali imprese, associazioni di categoria, università, ricerca, Pubblica Amministrazione, società civile, organizzazioni sindacali, terzo settore e associazioni dei consumatori, con l'obiettivo di elaborare una strategia nazionale in materia di tecnologie basate su registri distribuiti e *blockchain*. Il gruppo di esperti è stato designato al fine di individuare iniziative, *use cases* abilitanti e buone prassi esistenti, elaborare strumenti per creare e favorire condizioni economiche, politiche e regolatorie, individuare gli strumenti tecnici e normativi volti a diffondere l'applicazione degli *smart contracts* e fornire indirizzi strategici e modelli di *governance*.

4. La *blockchain* ed i c.d. "*Smart Contracts*".

Lo sviluppo degli *smart contracts* è andata di pari passo con l'evolversi ed il diffondersi della tecnologia *blockchain*[110], rappresenta la nuova frontiera della c.d. "*legal tech*", intesa come la combinazione della fenomenologia giuridico-legale con i più recenti ritrovati tecnologici[111]. Questa moderna tecnologia, infatti, ha offerto, oggi, uno strumento per rendere più agevole l'attuazione dell'interesse dei

[109] Cfr. Art. 8 *ter*, commi terzo e quarto, decreto legge n. 135/2018, convertito in legge n. 12/2019.
[110] Cfr. BATTELLI E., INCUTTI E.M., *Gli smart contracts nel diritto bancario tra esigenze di tutela e innovativi profili di applicazione*, in *Contratto e Impresa*, 2019, fasc. 3, p. 925; CRISCI S., *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro Amministrativo*, 2017, fasc. 10, pp. 1787 ss.;
[111] Cfr. GIULIANO M., *La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio*, cit. pp. 989 ss., spec. par. 4.1.

contraenti ad adottare un regolamento contrattuale flessibile e facilmente adattabile alle circostanze e alle esigenze contingenti[112].

Lo *smart contract* – o "contratto intelligente" – è stato per la prima volta[113] definito, come "un insieme di promesse, espresse in forma digitale, incluse le regole che le parti vogliono applicarvi", incorporate nell'*hardware* e nel *software* al fine di renderne impossibile o comunque eccessivamente oneroso l'inadempimento[114]. Esso nasceva come un protocollo informatico capace di incorporare, in sostanza, una serie di clausole contrattuali al proprio interno. La sfida che si è inteso perseguire mediante l'elaborazione di questo sistema è quella di rendere automatica l'esecuzione delle prestazioni contrattuali e, di fatto, impossibile il loro inadempimento[115].

Invero, l'aggettivo "*smart*" è ormai invalso nel gergo colloquiale quale termine per qualificare prodotti e servizi tecnologici in grado di migliorare la qualità della vita. Di derivazione anglosassone, esso, letteralmente, può essere tradotto in italiano con il termine "intelligente", ossia capace di determinate abilità e, in particolare, della facoltà di reagire a stimoli interni ed esterni[116]. Inserendolo nell'ambito contrattuale, nell'espressione, anch'essa di matrice inglese, "*smart contract*", serve, appunto, per indicare l'idoneità del vincolo negoziale ad auto eseguirsi senza necessità dell'intervento umano[117].

---

[112] Cfr. DI SABATO D., *Gli smart contracts: robot che gestiscono il rischio contrattuale*, cit., p. 378.

[113] Il termine *smart contract* è stato coniato per la prima volta negli anni '90 da Nick Szabo, un informatico statunitense, il quale aveva condotto numerosi studi legali e di crittografia. L'Autore, infatti, muovendo dall'idea per cui il contratto è "*a set of promises agreed to in a «meeting of the minds»*" era giunto ad affermare che "*the basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher*". Cfr., sul punto, SZABO N., *Smart Contracts: Building Blocks for digital markets*, in *http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html*, 1996, p. 1.

[114] In particolare, lo *smart contract* è stato definito come un "*computerized transaction protocol that executes the terms of a contract*" e, dunque, come un "insieme di promesse". Cfr., sul punto, SZABO N., *Smart Contracts: Building Blocks for digital markets*, cit., pp. 2 ss.

[115] Cfr. BATTELLI E., INCUTTI E.M., in *Gli smart contracts nel diritto bancario tra esigenze di tutela e innovativi profili di applicazione*, cit., p. 925.

[116] Sul punto, tuttavia, v. le critiche di FINOCCHIARO G., *Riflessioni sugli smart contract e sull'intelligenza artificiale*, in *Giustiziacivile.com*, 16 novembre 2020, ad avviso della quale i c.d. *smart contract*, in realtà a ben vedere, non sono né *smart* né *contract.*

[117] Cfr. CLACK C.D., BAKSHI V.A., BRAINE L., *Smart Contract Templates: foundations, design landscape and research directions*, in *arXijv.org*, 2016; SALITO G., voce *Smart Contracts*, cit., pp. 393-400.

Da un punto di vista giuridico, l'attenzione per la figura degli *smart contracts*, da parte dei giuristi, è, invece, relativamente recente ed è stata, senza dubbio, influenzata dal ruolo preponderate che, nella vicenda, riveste l'informatica, da cui lo *smart contract* deriva il carattere di "accordo automatizzato ed eseguibile. Automatizzato da un *computer*, sebbene alcune parti richiedano un *input* o un controllo umano. Eseguibile sia attraverso il ricorso all'autorità giudiziaria che tramite l'esecuzione automatica del codice"[118].

4.1. (*Segue*) Il funzionamento dello *smart contract*.

In altre parole, possiamo definire lo *smart contract* come un insieme di clausole, espressione di un accordo tra due o più parti, che sono programmate in codice alfanumerico. Il "codice" prefigura un *set* di istruzioni con la descrizione di condizioni all'avverarsi delle quali vengono automaticamente innescate specifiche azioni anch'esse definite nel codice. Il codice viene conservato sul *blockchain* così come le transazioni sono conservate normalmente su altre catene di controllo. L'impulso che determina l'esecuzione delle istruzioni registrate nello *smart contract* può dipendere da elementi interni allo stesso e, cioè, dalla successione di avvenimenti già compresi nel codice – come, ad esempio, lo spirare di un termine – ovvero da circostanze esterne – per esempio, un tasso di interesse –.

In tale seconda ipotesi è necessario l'intervento di un elemento esterno alla *blockchain* (c.d. "oracolo") che costituisce un collegamento tra la catena e il mondo reale e permette la verifica del soddisfacimento delle condizioni esterne. Si tratta, cioè, di un *software* che funziona quale un "informatore" avendo il ruolo di trasferire allo *smart contract* determinati dati provenienti dall'esterno della *blockchain* – come, ad esempio, il raggiungimento di un prezzo di quotazione di un titolo di borsa – al fine di verificare l'avveramento della condizione codificata nello *smart contract*[119]. L'oracolo, dunque, viene a rappresentare una fonte di dati affidabile e certificata che fornisce supporto per l'esecuzione o la non esecuzione

[118] Cfr. CLACK C.D., BAKSHI V.A., BRAINE L., *Smart Contract Templates: foundations, design landscape and research directions*, cit.
[119] Cfr. SARZANA F., *La Blockchain*, cit., pp. 95 ss.

dello *smart contract*, trasmettendo alla *blockchain* informazioni relative al mondo reale che concernono circostanze dedotte nel codice quali presupposti per l'esecuzione del contratto.

Di talché, a differenza di una catena di controllo semplice, la quale è in congegnata per registrare solo le transazioni, lo *smart contract* aggiunge un codice auto-eseguibile con un ulteriore grado di complessità e di organizzazione. I protocolli, infatti, servono per verificare ed eseguire le clausole del contratto e monitorano l'esecuzione dello stesso. La tecnologia *blockchain* permette, quindi, per così dire, la "*self-enforceability*" del contratto: vengono cioè eseguiti automaticamente i termini e le condizioni dello stesso al verificarsi degli eventi predeterminati dalle parti e iscritti nel codice.

Gli *smart contract* si basano, come un diagramma di flusso, sulla logica "*if this then that*"[120]: una volta soddisfatte le condizioni descritte nel codice si attivano automaticamente delle specifiche azioni che non possono essere interrotte. Infatti, dato che il libro mastro di *blockchain* è immutabile, il codice – e così il contratto al quale esso si riferisce – può solo essere cancellato o modificato seguendo i termini definiti dal codice stesso. Quindi, a differenza di ciò che avviene per i contratti tradizionali, che offrono la possibilità di adempiere le prestazioni come stabilito nel contratto stesso o di rendersi inadempienti ed andare incontro alle relative conseguenze – come, ad esempio, la risoluzione per inadempimento –, tale opzione non è disponibile in uno *smart contract* dove l'adempimento del contratto è, per così dire, automatizzato e subordinato unicamente al verificarsi di determinati eventi sottratti alla volontà delle parti[121]. Gli *smart contract*, in altri termini, non possono rimanere inadempiuti: la loro è una esecuzione a prova di manomissione, *tamper proof*[122].

---

[120] Letteralmente significa che se (*if*) si verifica un presupposto (*this*), allora (*then*) consegue un risultato.

[121] Per questo motivo lo *smart contract* è stato accostato più volte alle c.d. *vending machine* (distributori automatici), dove, una volta innescato il processo mediante l'inserimento del denaro e la digitazione del codice prodotto, l'adempimento (come l'erogazione del prodotto) è automatico e irreversibile.

[122] Contraria a tale interpretazione è la teoria negoziale, secondo cui l'adempimento, per poter essere qualificato tale, deve essere accompagnato da una specifica volontà del debitore di adempiere (cioè dell'*animus solvendi*) e dall'accettazione del creditore.

L'espressione *smart contract* si presta, quindi, a ricoprire un duplice significato: da un lato, esso è atto a designare la capacità degli agenti *software* di eseguire automaticamente alcuni atti inerenti ad obbligazioni e diritti; dall'altro, si presta ad indicare le modalità e le forme in cui la volontà negoziale è espressa mediante il linguaggio informatico. Entrambe le definizioni ricorrono negli studi che, prima dell'entrata in vigore della Legge dell'11 febbraio 2019, n. 12, di conversione del decreto legge del 14 dicembre 2018, n. 135, gli Autori che si sono occupati dell'argomento hanno suggerito, descrivendo gli *smart contract* ora come "protocolli per computer attraverso i quali si formalizzano gli elementi di un rapporto (solitamente di scambio), in grado di eseguire autonomamente i termini programmati una volta soddisfatte le condizioni predefinite"[123], ora come "la traduzione e la trasposizione di un contratto in un codice digitale non modificabile" che consente "a) di verificare automaticamente il rispetto delle condizioni contrattuali originariamente pattuite; b) di impartire, sempre in automatico, i comandi necessari perché il contratto sia adempiuto"[124], ora, ancora, in modo più sintetico, come "programmi informatici che consentono di eseguire delle operazioni"[125].

Il legislatore, invece, dal canto suo, come abbiamo precedentemente detto, nell'art. 8 *ter* del decreto legge n. 135 del 2018, qualifica lo *smart contract* alla stregua di un "programma per operatore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse" e precisa che esso soddisfa "il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale".

Questa nozione, tuttavia, presta il fianco a più di una criticità, tanto sul piano tecnico, quanto su quello più prettamente giuridico.

Invero, per quanto concerne il piano tecnico, è criticabile l'incompletezza della definizione in ragione del riferimento alla sola componente *software*, posto

---

[123] Cfr. CUCCURU P., *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, cit., pp. 107 ss.
[124] Cfr. MATTIUZZO F., VERONA N., *Blockchain e smart contract: nuove prospettive per il rapporto di lavoro*, cit., pp. 236 ss.
[125] Cfr. CAGGIANO I.A., *Il contratto nel mondo digitale*, in *Nuova Giurisprudenza Civile Commentata*, 2018, fasc. 7-8, pp. 1152 ss.

che, invece, un "programma per elaboratore" richiede necessariamente la presenza di un dispositivo ulteriore, ossia la componente *hardware*, su cui lo *smart contract* viene programmato ad agire. Vi è, tuttavia, chi ha ritenuto che più che trattarsi di un punto di criticità, questo ben potrebbe corrispondere ad una chiara scelta del legislatore, il quale ha inteso così evitare che, attraverso una norma definitoria, venisse circoscritto ad ambiti normativamente predefiniti l'impiego degli *smart contracts*[126].

Per quanto attiene, invece, al piano del diritto, le espressioni utilizzate nell'art. 8 *ter* danno adito a diversi interrogativi inerenti la natura giuridica della figura. Da un lato, infatti, la norma discorre di "effetti predefiniti dalle parti", rinviando ad un momento di formazione dell'accordo antecedente logicamente alla conclusione alla conclusione dello *smart contract*; dall'altro, invece, conferisce a quest'ultimo il valore di fonte di vincolo giuridico, posto che il legislatore si è avvalso del verbo "vincolare", con scelta opinabile posto che l'esecuzione, intesa come adempimento, determina l'estinzione di una obbligazione e non già il suo sorgere[127].

In termini riassuntivi, dunque, lo *smart contract* si presenta come un contratto "digitale", in quanto le clausole contrattuali sono incorporate nel *software* sotto forma di codice; è un contratto "auto-eseguibile", nel senso che l'adempimento, essendo governato dagli *input* previsti nel codice, prescinde non solo dall'*animus solvendi* del debitore, ma persino dal comportamento delle parti; e, infine, è un contratto "irrevocabile", poiché una volta iniziato, il processo di esecuzione non può essere fermato o modificato. Proprio in considerazione di tali caratteristiche intrinseche di *enforcement* delle regole pattizie intervenute tra i contraenti di uno *smart contract* si è ritenuto di potersi usare la già citata espressione "*Code is Law*", quasi a voler qualificare quello degli smart contracts un autonomo ordinamento giuridico[128].

---

[126] Cfr. MANENTE M., *L. 12/2019 - Smart Contract e tecnologie basate su registri distribuiti. Prime note, Studio 1_2019*, cit., p. 3.

[127] Cfr. sul punto MANENTE M., *L. 12/2019 - Smart Contract e tecnologie basate su registri distribuiti. Prime note, Studio 1_2019*, cit., p. 6, il quale fa rilevare, pertanto, come il termine "esecuzione", menzionato dall'art. 8 *ter*, non vada inteso nel suo significato giuridico ma in quello tecnico di "avvio2 del programma informatico.

[128] Cfr. DE FILIPPI P., HASSAN S., *Blockchain Technology as a Regulatory Technology. From Code is Law to Law is Code*, 2016, in *http://firstmonday.org/ojs/index.php/fm/article/view/7113*. In

Va da sé, dunque, la netta differenza tra lo *smart contract* e il contratto informatico, quello, cioè, redatto in formato digitale e finalizzato, mediante la tecnica del *point and click*, ad assicurare l'acquisto di beni o servizi in un ambiente di e-commerce. Il primo[129], infatti, si caratterizza per la capacità intrinseca di verificare le clausole contrattuali convenute tra i contraenti e di assicurarne l'automatica esecuzione, impartendo i comandi necessari per il reciproco adempimento delle prestazioni una volta che i dati riferiti alle situazioni reali accadute corrispondano alle clausole astratte concordate[130]. Il secondo, invece, è un normale contratto, reso con forma elettronica e siglato con firma digitale[131].

In dottrina non è mancato chi ha ritenuto che gli *smart contracts* altro non fossero se non una evoluzione dei contratti telematici e dei contratti cibernetici. Se nel contratto telematico l'uso dell'elaboratore collegato alla rete *internet* costituisce il mezzo per trasmettere la proposta di un contratto e riceverne l'accettazione[132] e nel contratto cibernetico le parti esprimono la loro volontà nelle istruzioni del *software* lasciando all'agente elettronico la definizione del contenuto e l'eventuale integrazione o modifica contrattuale[133], nello *smart contract* l'uso della tecnologia *blockchain* caratterizza il contratto per la totale disintermediazione dal fattore umano attraverso un database condiviso, decentralizzato, distribuito, criptato, resistente alle manomissioni e ad esecuzione automatica[134].

---

particolare, gli Autori hanno ritenuto di poter affermare che lo *smart contract* assurgerebbe al livero di un vero e proprio ordinamento autonomo, con proprie regole e modalità di esecuzione, incorporato nel codice software che assurgerebbe in tal modo a "legge" tra le parti.

[129] Cfr. BIANCA M., *Diritto civile*, cit., pp. 301 ss., il quale definisce i "contratti dell'automazione" come quei contratti determinati dall'evoluzione, determinata dalle tecnologie impiegate, dei contratti telematici.

[130] Cfr. MATTIUZZO F., VERONA N., *Blockchain e smart contract: nuove prospettive per il rapporto di lavoro*, cit., pp. 236 ss.

[131] Cfr. SALITO G., voce *Smart Contracts*, cit., pp. 393-400.

[132] In particolare, nei contratti telematici, conclusi in forma elettronica (si tratterebbe dei *paperless contracts*), lo strumento telematico costituisce solo il veicolo della volontà di soggetti distanti. Cfr. FAUCEGLIA D., *Il problema dell'integrazione dello smart contract*, in *Contratti*, 2020, fasc. 5, p. 591.

[133] Nei contratti cibernetici, la volontà dei soggetti non è solo veicolata ma anche formata dall'elaboratore elettronico che, appunto, non si pone solo come strumento di incontro delle parti e di formazione del programma contrattuale, ma come strumento che determina la volontà dei soggetti. Cfr. FAUCEGLIA D., *Il problema dell'integrazione dello smart contract*, cit., p. 591.

[134] In tal senso, cfr. GIULIANO M., *La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio*, cit., pp. 989 ss., spec. par. 4.1; STAZI A., *Automazione contrattuale e "contratti intelligenti". Gli smart contract nel diritto comparato*, Torino, 2019; CUCCURU P., *Beyond bitcoin: an early overview on smart contracts*, in *International Journal of Law and Information Technology*, 25, 2017, pp. 179-195; MILLARD C., *Blockchain and law: incompatible codes?*, in *Computer Law & Security Review*, 34, 2018, pp. 843-846.

Inoltre, grazie alle caratteristiche in cui si connota lo *smart contract*, derivano una serie di vantaggi che contribuiscono a contraddistinguere il contratto intelligente rispetto a quello "tradizionale". Anzitutto, per quei contratti che richiedono la necessaria partecipazione di un terzo intermediario – si pensi, ad esempio, ai contratti stipulati per la fornitura di energia elettrica e gas, o alla stipula di polizze assicurative, alla compravendita di un bene immobile, alla concessione di una linea di credito, ecc. – la conclusione di un contratto sulla *blockchain* sostituisce la necessità di un terzo intermediario con una "validazione" distribuita, con conseguente risparmio di tempo e di riduzione di costi normalmente legati all'adempimento dell'accordo contrattuale e ciò riduce, se non azzerare del tutto, il rischio di inadempimento di controparte. Peraltro, la registrazione – irreversibile e immodificabile – dello *smart contract* sulla *blockchain*, lascia una traccia indelebile e trasparente della storia del bene oggetto del medesimo e diminuisce il rischio di danni derivanti da errori e frodi.

Per queste ragioni, nel corso del tempo, sono svariati i settori nei quali si è sperimentata l'applicazione pratica degli *smart contract*. Per esempio, un primo esempio di *smart contract* nella storia dell'*e-commerce* è rappresentato da *eBay*, creato nel 1995, per gestire un sistema di compravendite e aste tramite procedure automatizzate in grado di attuare le clausole del contratto sottoscritto dai contraenti che vi aderiscono senza che questi entrino in contatto tra di loro. Non solo, ma gli *smart contract* possono, altresì, essere utilizzati nella fornitura e nel pagamento di energia elettrica: al consumo registrato dal contatore (che, in questo caso, rappresenta l'oracolo che collega il codice alla realtà esterna) ne consegue una bollettazione precisa ed un puntuale pagamento della fattura. Un secondo esempio è rappresentato dalla piattaforma "*UjoMusic*", che permette agli utenti di ascoltare musica e utilizzare i registri distribuiti per pagare direttamente gli artisti, senza ricorrere ad alcun tipo di intermediario. Infine, una ulteriore applicazione pratica dei contratti intelligenti in via di sviluppo riguarda la vendita di beni a rate: in una vendita a rate di un'autovettura, ad esempio, è stata ipotizzata una codificazione

contrattuale che permette di avviare il motore solo dietro il pagamento della rata nel termine pattuito[135].

4.2. (*Segue*) La qualificazione giuridica degli *smart contracts*.

Sono diversi i quesiti che gli *smart contracts* hanno posto, soprattutto dal punto di vista della loro qualificazione giuridica. Ci si è, infatti, chiesti quale sia, anzitutto, la relazione intercorrente tra l'accordo contrattuale ed il protocollo informatico (o codice) sotteso allo *smart contract* e, di conseguenza, quale valore possono assumere in ordine alla formazione ed esecuzione del contratto.

Da un lato, vi è chi ha ritenuto che gli *smart contracts* ben possano sostituirsi integralmente ai contratti i contratti tradizionali, con la conseguenza che il codice che si traduce nello *smart contract* possa costituire a tutti gli effetti il contratto. Di talché, il codice verrebbe ad avere forza di legge tra le parti ai sensi dell'art. 1372 Cod. Civ. e sarebbe, quindi, autosufficiente, auto-eseguito e autoimposto, senza alcuna possibilità di controllo da parte della giurisdizione nazionale[136], con la conseguenza che qualsiasi errore, clausola illegale o mancato recepimento di norme imperative diventerebbe parte del contratto, posto, appunto, che lo stesso viene ad essere sottratto ad ogni tipo di controllo esterno[137].

Questa interpretazione, tuttavia, pone il fianco ad almeno due ordini di critiche di difficile superamento. Invero, il primo dubbio che si pone inerisce, anzitutto, alla sua stessa struttura di programma destinato ad operare, come abbiamo già detto, su una *blockchain* e ad auto-eseguirsi, per effetto di un algoritmo di consenso e di una funzione crittografica di *hash*, che rende non invertibile l'operazione. Orbene, tanto l'algoritmo quanto la funzione importano una

---

[135] Un simile schema ben si colloca nell'alveo delle diverse forme di autotutela previste nel nostro ordinamento, quali, ad esempio, l'eccezione di inadempimento *ex* art. 1460 c.c., il potere di sospendere l'esecuzione in caso di mutamento delle condizioni patrimoniali di controparte *ex* art. 1461 c.c., e il diritto di ritenzione previsto dagli artt. 2756 e 2761 c.c.

[136] Si pensi, ad esempio, ad un obbligo di pagare una certa somma in un dato termine. Tale obbligo potrà essere soddisfatto creando uno *smart contract* (che essendo attestato su *blockchain* ha anche un proprio indirizzo univoco) dotato del relativo ammontare di valuta, il quale alla data prestabilita effettuerà il trasferimento della stessa verso il beneficiario.

[137] Cfr. PAROLA L., MERATI P., GAVOTTI G., *Blockchain e smart contract: questioni giuridiche aperte*, cit., pp. 681 ss.

formulazione basata su *templates*, ossia, su rappresentazioni elettroniche di documenti legali contenenti sia una parte in prosa che dei parametri, che rispondono alla logica dell'*if this then that*. È, dunque, il *coding* – ossia la programmazione informatica – a consentire di tradurre in gergo eseguibile tramite *computer* le specifiche azioni che le parti devono porre in essere in attuazione del contratto e le eventuali ed ulteriori regole rilevanti solo sul piano comportamentale. In ragione di tali caratteristiche lo *smart contract* non può essere ricondotto *tout court* al contratto[138]. Al contrario, sarà necessario distinguere il caso in cui il mezzo informatico sia funzionale unicamente alla trasmissione e alla successiva esecuzione dell'accordo contrattuale che si è perfezionato al di fuori di esso, secondo le modalità classiche, dal caso in cui l'accordo si formi direttamente attraverso il mezzo informatico, il quale provvede, altresì, alla sua trasmissione. Invero, nel primo caso, lo *smart contract*, lungi dall'essere una mera ripetizione negoziale di una dichiarazione già perfezionata *aliunde*, anziché essere esso stesso l'accordo, assume, invece, natura di strumento per la conclusione e gestione degli accordi. Nella seconda ipotesi, al contrario, esso integra un contratto se e nella misura in cui dello stesso contenga gli elementi essenziali individuati all'art. 1325 Cod. Civ.[139].

In secondo luogo, anche se si opera in *blockchain*, non si possono certamente legittimare accordi che siano in contrasto con le norme di diritto applicabili, anche se gli accordi che essa consente di creare sono automaticamente eseguibili. Il meccanismo di esecuzione automatica, invero, va considerato solamente come un mero strumento agevolatore per l'esecuzione del contratto in determinate ipotesi, ma ciò non toglie che, qualora il contratto sia invalido in base alle norme di legge ad esso applicabili, ciò darà diritto alla ripetizione delle prestazioni eseguite secondo i criteri ordinari. In tale ottica, quindi, gli *smart contract* devono certamente ritenersi soggetti alle norme di un determinato Stato o di una convenzione internazionale, individuate secondo i criteri di diritto internazionale privato[140].

---

[138] Cfr. SALITO G., voce *Smart Contracts*, cit., pp. 393-400.
[139] Cfr. CUCCURU P., *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, cit., pp. 107 ss.
[140] Cfr. SARZANA F., *La Blockchain*, cit., pp. 95 ss.

In dottrina, vi è, invece, chi ha ritenuto che agli *smart contracts* andrebbe riconosciuto il ruolo di mera automazione dell'adempimento, con la conseguenza che gli unici vantaggi derivanti dall'utilizzo di tali forme di intelligenza artificiale sarebbero unicamente riconducibili alla digitalizzazione e all'automatizzazione dell'adempimento al verificarsi di determinati eventi.

Più precisamente, gli *smart contracts* ben potrebbero essere collocati all'interno del sistema giuridico tradizionale, rilevando come unica differenza la sussistenza di una discrepanza tra l'accordo delle parti e il protocollo codificato, con la conseguenza che essi andrebbero integrati con ulteriori elementi espressione dell'intenzione e della volontà delle parti. Questa interpretazione – nota come c.d. *split contracting model* – ha il merito di cogliere due aspetti degli *smart contract*, ossia, da un parte, il vantaggio che dal loro uso ne deriva in termini di aumento di efficienza in molti settori, in quanto contribuirebbe a ridurre, ad esempio, i costi di transizione ed i tempi di necessari per lo svolgimento di attività di verifiche o controlli; dall'altra parte, invece, sottolinea l'incapacità e la difficoltà di tradurre in un unico codice complesse strutture negoziali[141].

Di talché, lo *smart contract* andrebbe ricondotto non alla fase di formazione del contratto – che è (e resta) costituita dall'accordo tra le parti –, bensì a quella dell'adempimento, con la conseguenza che lo *smart contract* non potrebbe, di fatto, integrare neppure una fattispecie di contratto atipico ai sensi dell'art. 1322 Cod. Civ. D'altro canto, se, da un lato, l'autonomia contrattuale viene senz'atro garantita nel momento di formazione del contratto, dall'altro lato, la stessa viene limitata in relazione alla fase dell'adempimento.

[141] Cfr. PAROLA L., MERATI P., GAVOTTI G., *Blockchain e smart contract: questioni giuridiche aperte*, cit., pp. 681 ss.

CAPITOLO SECONDO

La tutela della *privacy* nell'era digitale

SOMMARIO: 1. Il diritto all'identità personale. – 1.1. (*Segue*) L'identità nell'era di Internet: la c.d. "identità virtuale". – 1.2. (*Segue*) La tutela dell'identità in rete ed il diritto all'oblio. – 2. Il concetto di "dati personali" nella società dell'informazione. – 2.1. (*Segue*) La commercializzazione e la protezione dei dati personali. – 3. L'origine del concetto di "*Privacy*". – 3.1. (*Segue*) Il contributo della dottrina nazionale sull'individuazione del concetto di "*privacy*". – 3.2. (*Segue*) Il contributo della giurisprudenza nazionale sul concetto di *privacy*. – 3.3. (*Segue*) Le fonti in ambito comunitario in tema di riservatezza. – 3.4. (*Segue*) L'evoluzione normativa degli ordinamenti europei in tema di tutela della *privacy*. – 4. La tutela della *privacy* nell'era digitale.

1. Il diritto all'identità personale.

Il diritto alla identità personale è un diritto di creazione giurisprudenziale[142], per la cui definizione la dottrina ha, tuttavia, rivestito un ruolo preponderante, risalendo già agli inizi degli anni '50 i primi contributi in materia che gli Autori

[142] Cfr., in particolare, DE CUPIS A., *Bilancio di un'esperienza: diritto all'identità personale*, in AA.VV., *La lesione dell'identità personale e il danno non patrimoniale. Atti del seminario promosso dal Centro di iniziativa giuridica P. Calamandrei*, Messina, 16 aprile 1982, Milano, 1985, p. 189; DE CUPIS A., *La verità nel diritto*, in *Foro Italiano*, 1952, fasc. IV, p. 223; ZENO ZENCOVICH V., «*Identità personale*», in *Digesto delle discipline civilistiche*, IX, Torino, 1995, p. 295, il quale, in particolare, ricorda la circostanza significativa che talora i teorici del diritto all'identità personale hanno rivestito anche il ruolo di giudici nelle controversie concernenti proprio la definizione di tale diritto.

hanno dato. Si tratta, invero, di un aspetto della personalità di più recente emersione rispetto agli altri, identificato con l'interesse del soggetto "ad essere se stesso", ad affermare "nella vita di relazione" una "verità attinente alla persona"[143]. Esso, infatti, è stato costruito come un diritto autonomo[144], slegato dagli altri diritti della personalità, come il diritto al nome e all'onore[145], ed è stato inteso come il diritto a che non sia travisata la propria immagine politica, etica o sociale con l'attribuzione di azioni non compiute dal soggetto o di convinzioni da lui non professate.

Si trattava, all'inizio, di un diritto non ancora chiaramente contraddistinto rispetto alla tutela degli altri diritti della personalità, ma si è arricchito man mano grazie al progressivo approfondimento di aspetti diversi, giungendo alla definitiva descrizione come diritto soggettivo operato dalla dottrina[146], nonché dalla Corte di Cassazione nel 1985[147]. Da questo momento in poi, l'espressione "identità

---

[143] Cfr. BAVETTA G., *Identità (diritto alla)*, in *Enciclopedia del diritto*, XIX, Milano, 1970, p. 953.

[144] Cfr. GIACOBBE G., *L'identità personale tra dottrina e giurisprudenza. Diritto sostanziale e strumenti di tutela*, in AA.VV., *La lesione dell'identità personale e il danno non patrimoniale. Atti del seminario promosso dal Centro di iniziativa giuridica P. Calamandrei*, Messina, 16 aprile 1982, Milano, 1985, p. 14.
In realtà, parte della dottrina – sulle tracce di alcuni contributi più risalenti – esclude la configurabilità di un autonomo diritto, qualificando l'identità personale semplicemente come un bene diretto a soddisfare un interesse che l'ordinamento tutela solo attraverso singole specifiche norme relative ad altri diritti della personalità e, ciò, per il timore che una tutela generalizzata comprima eccessivamente la libertà di pensiero di cui all'art. 21 Cost. Cfr. PACE A., *Art. 15*, in G. Branca (a cura di), *Commentario della Costituzione italiana*, Roma-Bologna, 1977, pp.130 ss.; MACIOCE F., *Profili del diritto al nome civile e commerciale*, Padova, 1984, pp. 205 ss.; ARCESE G., *Riflessioni sull'"autonomia" del diritto all'identità personale,* nota a P. Roma, (ord.) 7 gennaio 1984, in *Rassegna di Diritto Civile*, 1985, pp. 225 ss., il quale àncora il diritto all'identità personale al solo diritto di rettifica; MASTROPAOLO E., *Identità personale e manifestazione del pensiero. Strumenti di tutela*, in *Diritto Informatico e dell'Informatica*, 1985, pp. 561 ss.

[145] Cfr. ZENO-ZENCOVICH V., *Identità personale*, cit., p. 295.

[146] In tal senso cfr. GIACOBBE G., *L'identità personale tra dottrina e giurisprudenza. Diritto sostanziale e strumenti di tutela*, in AA.VV., *La lesione dell'identità personale e il danno non patrimoniale. Atti del seminario promosso dal Centro di iniziativa giuridica P. Calamandrei*, cit., pp. 810 ss. Contra ARCESE G., *Riflessioni sull'autonomia" del diritto all'identità personale*, cit., pp. 225 ss., il quale connette il diritto all'identità personale al solo diritto di rettifica. Sul punto cfr., altresì, ROPPO E., *Diritti della personalità, diritto all'identità personale e sistema dell'informazione. Quale modello di politica del diritto?*, in Alpa, Bessone, Boneschi, Caiazza (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983. In particolare, l'Autore ritiene che sia utile la distinzione fra diritti della personalità come pretesa alla limitazione di poteri o comportamenti altrui, e diritto all'identità personale come pretesa del soggetto ad essere se stesso, ma ritiene non debba trattarsi di contrapposizione, ma di individuazione di due diverse dimensioni e due diversi valori.

[147] Cfr. Corte di Cassazione, sentenza del 22 giugno 1985, n. 3769, in *Diritto dell'Informazione e Informatica*, 1985, p. 965. Nel 1985, infatti, i giudici di legittimità si sono pronunciati sul diritto alla personalità e lo hanno fatto in occasione del "caso Veronesi": l'oncologo aveva infatti citato in giudizio una società produttrice di tabacco (*Austre Tabawerke*) dal momento che la stessa, in un inserto pubblicitario finalizzato alla promozione di sigarette "leggere", aveva manifestamente travisato alcune dichiarazioni del Veronesi che, in occasione di un'intervista – dietro espressa domanda del giornalista – aveva riferito che sul mercato esistono effettivamente sigarette meno

personale" è stata sempre più spesso menzionata, ed è stata specificata come diritto, finendo con l'entrare a pieno titolo nel novero degli aspetti della personalità tutelati dall'ordinamento, accanto a quelli (nome, immagine, reputazione) positivamente previsti, o comunque di lunga tradizione dottrinaria (come, appunto, la *privacy*), anche se spesso la relativa protezione è stata accordata mediante il richiamo ad altri aspetti dei diritti della personalità o anche in connessione con essi.

Tuttavia, il diritto all'identità personale, nel corso del tempo, è venuto differenziandosi dalle altre situazioni giuridiche soggettive affini, per avere ad oggetto quello specifico bene-valore costituito dalla proiezione sociale della complessiva personalità dell'individuo, alla base del quale si colloca l'interesse del soggetto ad essere rappresentato – nella vita di relazione – con la sua vera identità e, cioè, a non vedere modificato, offuscato o, comunque, alterato all'esterno il proprio patrimonio intellettuale, ideologico, politico, etico, religioso, professionale ecc., come già estrinsecatosi (o destinato comunque ad estrinsecarsi) nell'ambiente sociale[148].

Orbene, il termine "identità" può assumere una varietà di significati, in relazione al contesto (sociale, politico, economico) in cui lo stesso è utilizzato, alla problematica cui viene affiancato, alla persona che cerca di rappresentare. Invero, la figura può avere una duplice connotazione, personalistica ed individualistica, da

---

nocive di altre ma non per questo "salutari", il professore infatti, storico promotore di un'intensa campagna educativa antifumo, aveva concluso dicendo "tutto certamente sarebbe più semplice se la gente si convincesse a non fumare". Ciononostante, la *Austre Tabawerke*, nel promuovere il proprio prodotto, aveva adoperato le seguenti parole: "Secondo il prof. Umberto Veronesi - direttore dell'Istituto dei tumori di Milano - questo tipo di sigarette riducono quasi della metà il rischio del cancro". La domanda giudiziale formulata dal Prof. Veronesi aveva a fondamento non già solo la lesione del diritto al nome e all'immagine dell'oncologo ma anche e soprattutto del diritto alla sua identità personale; le pretese del medico, seppur con diverse argomentazioni, venivano accolte sia in primo che in secondo grado.

Ancora prima di questo arresto giurisprudenziale, in realtà, il diritto all'identità personale è stato definito con la storica sentenza della Pretura di Roma del 6 maggio 1974 in *Giurisprudenza Italiana,* 1975, fasc. I, 2, p. 514, come il diritto a «non vedersi travisare la propria personalità individuale». Invero, in tale occasione, il pretore romano ha per la prima volta prestato tutela all'interesse dei ricorrenti a non vedersi attribuite indebitamente idee e posizioni politiche estranee alle proprie credenze e convinzioni. Tale pronuncia si è posta in netta rottura rispetto all'orientamento giurisprudenziale prevalente secondo cui "nessuna norma, o complesso di norme prevede una situazione di diritto soggettivo che abbia come contenuto il potere di pretendere il rispetto della verità storica della persona, verità questa che potrebbe trovare garanzia solo indirettamente, ovvero nell'ipotesi in cui a essere lesi siano valori giuridicamente rilevanti o nel caso in cui vi sia un'espressa previsione legislativa".

[148] Cfr. Corte di Cassazione, sentenza del 7 febbraio 1996, n. 978, in *Corriere giuridico*, 1996, fasc. 3, p. 264.

un lato, e sociale e relazionale, dall'altro: dall'essere identificati con un nome ed un cognome, all'essere ritratti con una propria immagine; dall'essere presenti in un dato momento storico, all'essere individuati con un preciso pseudonimo; dall'apparire agli occhi degli altri per quello che si è, al voler figurare all'esterno per quello che si vuole far vedere di sé[149]. Non è rilevante l'identità intesa in senso soggettivo, come opinione che il soggetto abbia del proprio "io", bensì in senso oggettivo, con riferimento alla personalità dell'individuo percepita o percepibile – nella realtà sociale – grazie alle normali diligenza e buona fede soggettiva ed in base a riscontri obiettivi e comportamenti espliciti. Si parla, a tal proposito, di c.d. "dimensione relazionale" dell'identità personale[150].

Il concetto di identità personale, dunque, può essere inteso come il punto di incontro tra il concetto di soggetto e il concetto di persona nella sua rappresentazione sociale e nelle sue espressioni ideali. Per questo esso rappresenta una formula sintetica per contraddistinguere il soggetto dal punto di vista globale nella molteplicità delle sue specifiche manifestazioni. Invero, in giurisprudenza si è sottolineato che "il relativo diritto richiama l'esigenza di essere se stessi, nella prospettiva di una compiuta rappresentazione della personalità individuale in tutti i suoi aspetti ed implicazioni, nelle sue qualità ed attribuzioni; diritto alla propria identità, sottoposta ai medesimi mutamenti della personalità individuale (e quindi diritto "alla personalità" e alle condizioni che ne garantiscono lo sviluppo)"[151].

La disposizione normativa solitamente utilizzata per fondare il diritto all'identità personale è stato l'art. 2 Cost., posto che la sua formula "diritti inviolabili", la connota come disposizione aperta che ha consentito di ampliare il catalogo dei diritti fino a quel momento esistenti. Come sostenuto in dottrina, infatti, "il diritto all'identità personale ha per oggetto l'interesse della persona all'intangibilità della propria proiezione sociale e al vedersi riconoscere all'esterno il proprio patrimonio intellettuale o culturale"[152].

Il diritto all'identità personale ha, poi, trovato esplicita menzione legislativa sia nella legge n. 675 del 1996 sul trattamento dei dati personali, poi confluita, come

[149] Cfr. RUSSO P., *I danni esistenziali*, Torino, 2014, p. 476.
[150] Cfr. ALPA G., *Giurisprudenza di merito* 84, IV, p. 471.
[151] Cfr. Corte di Cassazione, sezione I, sentenza del 15 dicembre 2011, n. 27069, *www.personaedanno.it.*
[152] Cfr. CENDON P. (a cura di), *Il quantum nel danno esistenziale*, Milano, 2010, p. 482.

vedremo, unitamente ad altri provvedimenti normativi stratificatisi nel tempo, nel Codice in materia di protezione dei dati personali, ossia il decreto legislativo n. 196 del 2003, che all'art. 2, primo comma, "garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

1.1. (*Segue*) L'identità nell'era di *Internet*: la c.d. "identità virtuale".

Il concetto di identità personale si è connotato, soprattutto negli ultimi anni, per essere un concetto in veloce evoluzione, avendo risentito delle modifiche normative e della nuova teorizzazione dei diritti della personalità causate dallo sviluppo dell'informatica e della telematica che, cambiando relazioni e prospettive, ha modificato conseguentemente i rapporti giuridici e causato l'evoluzione normativa[153].

Discorrere di identità personale, oggi, invero, significa fare i conti anche con una nuova dimensione, ossia quella informatica, nella quale l'identità personale risulta indispensabile per il compimento di una serie di azioni, per lo più di carattere patrimoniale; per farsi un'idea di quanto detto è sufficiente pensare all'utilizzo delle carte di credito sul *web*, alle varie transazioni commerciali, fino ad arrivare ai *social network*[154].

Occorre anche considerare che *Internet* consente all'individuo di manifestare la propria identità in varie forme, "in condizioni di assoluta democrazia e uguaglianza"[155]. Esso, infatti, rappresenta il luogo nel quale la connessione tra i dati consente di ridisegnare il concetto, cambiandolo e a volte deformandolo rispetto all'originale valenza, ossia quella reale, arrivando, sovente a disgregare la stessa identità personale[156]. E, tutto ciò, avviene, come sottolineato dalla dottrina,

---

[153] Cfr. RODOTÀ S., *Quattro paradigmi per l'identità*, in *Vivere la democrazia*, Bari, 2018, pp. 20 ss.
[154] Cfr. ALPA G., *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impresa*, 2017, p. 725
[155] Cfr. CASSANO G., CONTALDO A., *Diritti della persona, internet e responsabilità dei soggetti intermediari*, in *Corriere giuridico*, 2010, p. 16
[156] Cfr. ALPA G., *L'identità digitale e la tutela della persona. Spunti di riflessione*, cit., p. 725.

con due caratteristiche importanti: "velocità" e "a-territorialità"[157], posto che nel mondo virtuale, le coordinate di spazio e tempo, come già accennato, vengono annullate in favore di una maggiore "possibilità di conservare, comunicare e trasmettere le informazioni e il sapere"[158].

Il *web* contiene una memoria immensa, universale, ma anche disorganizzata e volatile, "riduce lo scarto temporale tra produzione e l'utilizzazione del sapere"[159], con la conseguenza che l'identità personale finisce con il sembrare frammentata, "inconoscibile" ed "instabile"[160]. Ogni utente può "creare e condividere un'informazione" e "determinarne la diffusione e moltiplicazione esponenziale in tempi molto ridotti"[161]. Il classico esempio di quanto detto è rappresentato dal c.d. fenomeno della "viralità" di video o foto o informazioni, che sovente determinano in capo al soggetto che ne è vittima una lesione grave.

La rivoluzione digitale ha, dunque, portato un cambiamento radicale nel modo di intendere l'individualità, apparendo, ora, essa alla stregua di un "complesso di dati tradotti in algoritmi"[162].

Già nella legge n. 675 del 1996, come vedremo, il soggetto viene rappresentato come titolare dei dati costituiti da "qualunque informazione relativa a persona fisica [...] identificabile anche indirettamente mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"; aggiunge, poi, l'art. 4 del Regolamento europeo n. 679 del 2016 anche il riferimento a "qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato')"; *ivi* precisandosi che "si considera identificabile la persona fisica che può essere [individuata], direttamente o indirettamente, con particolare riferimento a un [...] nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua

---

[157] Cfr. CASSANO G., CONTALDO A., *Diritti della persona, internet e responsabilità dei soggetti intermediari*, cit., p. 16.
[158] Cfr. MARTINELLI S., *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in internet e le problematiche poste dalla de-indicizzazione*, in *Diritto dell'informatica*, 2017, p. 566.
[159] MARTINELLI S., *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in internet e le problematiche poste dalla de-indicizzazione*, cit., p. 566.
[160] Cfr. RODOTÀ S., *Il diritto di avere diritti*, Roma-Bari, 2012, p. 173.
[161] Cfr. MARTINELLI S., *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in internet e le problematiche poste dalla de-indicizzazione*, cit., p. 567.
[162] Cfr. ALPA G., *Tecnologie e diritto privato*, in *Rivista italiana per le scienze giuridiche*, 2017, p. 276.

identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". In tal senso, dunque, il Regolamento "allude ad altri diritti fondamentali o costituzionalmente garantiti, la cui protezione si associa a quella della protezione della persona riguardo al trattamento dei dati: si pensi al nome (art. 22 Cost.), allo pseudonimo (*ex* art. 22 Cost.), all'immagine (*ex* art. 2 Cost.) e agli altri aspetti della identità"[163].

Si tratta nella sostanza di situazioni soggettive che vanno ad aggiungersi ai diritti della personalità ormai tradizionali e che "ampliano lo spettro delle posizioni giuridiche soggettive e creano dunque potenziali conflittualità"[164]. Invero, la libera raccolta ed utilizzazione di informazioni e dati "può implicare danni alla persona, ledere cioè la sua immagine, il suo nome, la sua identità, la sua riservatezza"[165]. Di talché, sorge l'obbligo di far rispettare in ambito virtuale, non solamente i tradizionali diritti della personalità, ossia il diritto al nome, all'immagine, all'onore, alla reputazione, ma anche i "nuovi" diritti alla riservatezza, all'identità personale, all'oblio[166].

Ecco perché, oggi, si parla sempre più spesso di "identità digitale" come sinonimo di identità "in rete" o "virtuale". Da un punto di vista informatico, tali espressioni servono a riassumere in un'unica nozione i sistemi che individuano delle credenziali di accesso a risorse informatiche allo scopo di collegarle, almeno di norma, ad una persona fisica, in modo spesso univoco[167]. Da un punto di vista giuridico, invece, benché alcuna normativa sul punto sia ancora stata introdotta, possiamo ritenere che l'identità digitale costituisca l'"insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utente utilizzatore del suddetto sotto un processo di identificazione"[168].

Invero, l'espressione sovente usata dalla dottrina, secondo cui "siamo un complesso di dati" si riferisce proprio all'idea di un individuo considerato per i suoi

---

[163] Cfr. ALPA G., *La "proprietà" dei dati personali,* in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, Milano, 2019, p. 17.
[164] Cfr. ALPA G., *La "proprietà" dei dati personali*, cit., p. 17.
[165] Cfr. ALPA G., *La "proprietà" dei dati personali*, cit., pp. 280 ss.
[166] Cfr. CASSANO G., CONTALDO A., *Diritti della persona, internet e responsabilità dei soggetti intermediari*, cit., p. 16.
[167] Cfr. NASTRI M., *Identità personale, identità digitale e identificazione elettronica alla luce del decreto semplificazioni*, in *Notariato*, 2020, fasc. 6, p. 608.
[168] Cfr. RESTA G., *Identità personale e identità digitale*, in *Il Diritto dell'Informazione e dell'Informatica*, 2007, p. 515.

dati personali e, il dato personale, in quanto strettamente legato alla persona, ne compone l'identità digitale, quasi fosse una proiezione della persona stessa, "una sua parte"[169].

Il problema di fondo è che i dati consentono al soggetto di costruire diverse identità in rete: l'immagine che un soggetto sceglie di proiettare nel mondo di internet, realtà virtuale, infatti, può coincidere o meno con quella reale. Già lo stesso utilizzo di un c.d. "*nickname*" gli consente di ricorrere all'impiego di nomi fittizi, diversi da quelli effettivi. Così facendo, potrà risultare piuttosto semplice avere un'identità parallela su *Internet*, fino all'anonimato, o un'identità digitale coincidente con quella elettronica, attraverso l'identificazione a mezzo firma digitale.

Orbene, "il diritto all'identità digitale attiene all'interesse della persona alla non manipolabilità di quello che rappresenta virtualmente, vedendosi riconoscere in rete la propria peculiarità intellettuale, politica, sociale e religiosa, con l'interesse a non essere decontestualizzato pervenendo ad affermazioni contrarie a quanto costantemente affermato"[170]. Così inteso, dunque, il diritto all'identità digitale potrebbe finire con l'essere letto "come declinazione del diritto all'identità personale [...] specie del genere costituito dai diritti della personalità"[171].

Ma, sul punto, occorre fare una precisazione: l'identità digitale si differenzia dall'identità personale poiché essa è frammentata[172], "dispersa, per il fatto che le informazioni riguardanti la stessa persona sono contenute in banche dati diverse, ciascuna delle quali restituisce soltanto una parte o un frammento dell'identità complessiva"[173], nel senso che può essere il risultato di collegamenti con numerosi luoghi virtuali. Al contrario, l'identità personale è unitaria e la sua tutela risulta statica, affidata cioè ai tradizionali mezzi inibitori o risarcitori, successivi alla lesione. L'identità digitale, la protezione dei dati, invece, richiede una tutela

[169] Cfr. ALPA G., *La "proprietà" dei dati personali*, cit., p. 17.
[170] Cfr. CASSANO G., CONTALDO A., *Diritti della persona, internet e responsabilità dei soggetti intermediari*, cit., p. 5.
[171] Cfr. CASSANO G., CONTALDO A., *Diritti della persona, internet e responsabilità dei soggetti intermediari*, cit., p. 5.
[172] Sul punto cfr. tra i tanti, BAUMAN Z., *Intervista sull'identità*, Bari-Roma, 2009, pp. 87 ss.
[173] Cfr. ALPA G., *La "proprietà" dei dati personali*, cit., p. 173.

"dinamica, segue i dati nella loro circolazione", sotto forma di controllo della raccolta delle informazioni[174].

Proprio in virtù di quanto detto, l'identità digitale necessita di una tutela più ampia poiché il soggetto potrebbe non avere nessun controllo sulla rappresentazione di siffatta sua identità, che potrebbe essere formata automaticamente. Essa potrebbe essere imposta attraverso la strutturazione di "profili digitali" creati e basati su dati inseriti dal soggetto stesso e su algoritmi, che sfuggono al controllo del soggetto e che talvolta costruiscono la "personalità digitale" del soggetto medesimo, immaginando anche comportamenti futuri (si pensi alle preferenze di acquisto). Con la profilazione si individuano correlazioni di dati relativi a un soggetto, che non viene identificato, ma allo stato solo riconosciuto, ad esempio, mediante l'utilizzo dei c.d. *cookies*. Viene creato un profilo digitale, riferito ad un soggetto "potenziale", costruito automaticamente, di cui il soggetto non conosce il contenuto. Il profilo può anche coincidere con la effettiva identità digitale del soggetto, identità questa che si riferisce a un soggetto "reale", il quale è edotto dello scopo e ne conosce i contenuti. L'identità personale è sostanzialmente scevra da eteronomia, è sufficientemente nota, poggia su modelli socio-culturali, è il riflesso sociale del soggetto-persona[175].

1.2. (*Segue*) La tutela dell'identità in rete ed il diritto all'oblio.

Il diritto all'oblio è il diritto soggettivo, di matrice giurisprudenziale[176], emerso a cavallo tra gli anni Ottanta e Novanta del secolo scorso, a che una notizia – relativa al titolare di tale diritto ed in qualche modo, benché vera e confezionata

[174] Cfr. RODOTÀ S., *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy*, in *Europa e Diritto Privato*, 2004, p. 3. In questa direzione si muove la disciplina, dalla direttiva 46/96/CE al Codice della privacy, al Regolamento UE 679/2016.

[175] Cfr. MESSINETTI R., *Circolazione dei dati personali e autonomia privata*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, Milano, 2019, pp. 167 ss.

[176] Benché il legislatore non abbia fornito una compiuta definizione del diritto *de quo*, la giurisprudenza ha da tempo affermato che il nostro ordinamento riconosce il diritto soggettivo all'oblio. A tal proposito cfr., in particolare, Corte di Cassazione civile, sentenza del 9 aprile 1998, n. 3679, in *Foro Italiano*, 1998, fasc. I, p. 1834; Corte di Cassazione, sentenza del 18 ottobre 1984 n. 5259, in *Giurisprudenza italiano*, 1985, p. 762; Tribunale di Roma, sentenza del 15 maggio 1995, in *Diritto informatico e informatica*, 1996, p. 427; Corte di Cassazione penale, V sezione, sentenza del 24 novembre 2009, n. 45051, in *Studium Iuris*, 2010, n. 5, p. 577.

in modo appropriato, lesiva per la sua immagine o per altri suoi interessi protetti[177] – non sia resa oggetto di attenzione pubblica[178], e, dunque, non sia riproposta all'opinione pubblica, dopo un certo lasso di tempo dalla sua prima diffusione o dall'accadimento del fatto a cui la notizia si riferisce. Ciò, a patto che non sussista nella comunità di riferimento un interesse diffuso attuale per la notizia in questione, giacché in un simile caso il diritto all'informazione prevarrebbe sul diritto individuale all'oblio[179].

La nascita di un simile diritto, va da sé, si ricollega direttamente a quella che può definirsi come "società dell'informazione"; si tratta, infatti, di un diritto venuto in rilievo nel momento in cui – specialmente con l'avvento di Internet – ci si trovava nella situazione per cui una notizia, benché vera, e diffusa originariamente in modo corretto, potesse nel tempo arrecare disagio all'interessato[180].

Tale diritto, invero, si inserisce nel novero dei diritti della personalità che sorge in un momento in cui si riconosce all'interessato il potere di ottenere che, salvo eccezioni, accadimenti relativi alla sua vita passata, non più di interesse pubblico, fossero dimenticati, e cioè non fossero riproposti, a distanza di tempo, pubblicamente. Ciò che si vuole evitare, mediante il riconoscimento normativo di un diritto di tale portata, è ovviamente il rischio che si possa arrecare danno a qualcuno mediante la proposizione o riproposizione di vecchia notizia che non interessa più alla collettività.

---

[177] Spesso si è discusso nel corso degli anni sull'individuazione del soggetto legittimato ad invocare la tutela del diritto all'oblio. Infatti, mentre è scontato che tale legittimazione spetti al protagonista in negativo della vicenda, dubbi si sono posti rispetto all'analoga legittimazione in capo alla eventuale vittima o ai congiunti di questa. Sul punto cfr. DI CIOMMO F., *Quello che il diritto non dice. Internet e oblio*, in *Danno e Responsabilità*, 2014, fasc. 12, p. 1101.

[178] Con ciò intendendo, non solo la stampa, ma anche e principalmente *Internet*, e più in generale qualunque altro mezzo di informazione.

[179] Il riferimento è a quei fatti talmente gravi che l'interesse pubblico alla loro riproposizione pubblica non viene mai meno. È il caso, ovviamente, dei crimini contro l'umanità, per i quali riconoscere ai loro responsabili un diritto all'oblio sarebbe addirittura diseducativo.

[180] Nella dottrina italiana, i contributi sul diritto all'oblio sono molteplici. Cfr. tra gli altri, VIGEVANI G.E., *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano*, in *Danno e Responsabilità*, 2014, p. 731; MARCHETTI G., *Diritto di cronaca on-line e tutela del diritto all'oblio*, in AA.VV., in *Da Internet ai social network*, Sant'Arcangelo di Romagna, 2013, p. 71; DE GRAZIA L., *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso Internet: argomenti comparativi*, in *Rivista dell'Associazione Italiana dei costituzionalisti*, 2013, fasc. 4, p. 1; DI CIOMMO F., PARDOLESI R., *Dal diritto all'oblio in Internet alla tutela della identità dinamica. È la rete, bellezza!*, in *Danno e Responsabilità*, 2012, p. 701; FEROLA L., *Dal diritto all'oblio al diritto alla memoria sul Web. L'esperienza applicativa italiana*, in *Diritto dell'informatica*, 2012, p. 1001; FERRI G.B., *Diritto all'informazione e diritto all'oblio*, in Rivista di diritto civile, 1990, p. 801.

Va da sé che l'avvento e la rapidissima espansione della rete *Internet* ha reso molto complicato lo scenario, posto che, come più volte ribadito, oramai siamo tutti – cibernauti e non – inevitabilmente immersi in un flusso di informazioni continue, che si alimenta perennemente senza che sia più dato distinguere chi opera per alimentare il flusso e chi invece si limita ad usufruirne[181].

Oggi, infatti, chiunque, in rete può immettere informazioni, anche di carattere personale, riguardanti sé o terzi; *Internet* offre quotidianamente la possibilità di informarsi in tempo reale attraverso la semplice presenza *online*, la quale, di per sé sola, assicura la ricezione continua di informazioni di qualsiasi tipo e specie, attraverso i *social network* a cui si partecipa o, comunque, attraverso stringhe informative assicurate su molteplici siti. A ciò deve anche aggiungersi la considerazione per cui è semplicissimo per qualsiasi utente cercare, in vario modo, informazioni, attuali o non, su qualsiasi circostanza, persona o curiosità, posto che oramai le informazioni sono sempre sulla grande rete a disposizione di tutti, con la conseguenza che ogni utente può in qualsiasi momento entrare in contatto con una data notizia anche datata.

A corollario di quanto detto si pone anche il fatto che oggi *Internet* costituisce un'immensa banca dati, continuamente arricchita da milioni di informazioni immesse in rete ogni secondo, a carattere globale, senza soluzione di continuità, da chiunque voglia farlo. Si tratta di informazioni di ogni genere e contenuto. Da quelle pubblicate da giornalisti professionisti su siti che svolgono espressamente attività informativa, a quelle istituzionali, a quelle commerciali, fino a quelle, e sono la stragrande maggioranza, postate da semplici utenti sui siti più disparati e soprattutto, oggi, tramite i *social-network*, nei quali i cyber-utilizzatori inseriscono (normalmente senza porsi alcun problema di *privacy*) notizie, fotografie, comunicazioni e quant'altro, che riguardano loro o altri.

Di talché, oggi risulta particolarmente difficoltoso parlare ancora di oblio, identità, *privacy* e riservatezza, per come si è fatto nella seconda metà del XX secolo, destinata a scontrarsi quotidianamente con la più evidente ed elementare

[181] DI CIOMMO F., PARDOLESI R., *Dal diritto all'oblio in Internet alla tutela della identità dinamica. È la rete, bellezza!*, cit., p. 701.

realtà contraria[182]. Un qualunque dato caricato in *Internet* e reso disponibile ai naviganti, infatti, esce dalla sfera di esclusiva disponibilità dell'autore, ossia di colui che lo ha immesso in rete per primo, o del sito sorgente, ossia il primo sito nel quale quel dato è apparso, posta la facilità con la quale sia possibile copiarlo, memorizzarlo, per poi poter essere rintracciato mediante i c.d. "motori di ricerca"[183].

Qualsiasi dato, dunque, una volta immesso in rete, può essere riprodotto tante più volte quanto più interesse, per varie ragioni, suscita tra gli utenti; sicché tale dato alla fine potrà risultare presente in diversi siti e in diverse forme contemporaneamente e potrà rimanersi non per un giorno, una settimana o un anno, ma per sempre, o meglio sino a quando dal punto di vista tecnico ciò sarà possibile.

In definitiva può dirsi che "il diritto al controllo, che costituisce il cuore stesso del diritto all'identità personale, del diritto all'oblio, del diritto alla protezione dei dati personali, si infrange, al momento, sulla tecnica"[184] e la protezione del dato personale va letta, proprio, nell'ambito delle vicende dell'identità personale, del diritto a "non vedersi travisare la propria personalità individuale"[185].

I rimedi tecnologici per far fronte a questa situazione e per consentire una qualche forma di tutela sono diversi; per citarne alcuni, DRM – acronimo di "*Digital Rights Management*" –, cioè un rimedio in virtù del quale le informazioni associate ai dati personali recano in sé le regole di utilizzo dei dati stessi (ad esempio: natura, titolare, interessato, finalità); la scadenza nell'uso dei dati personali, nonché, la contestualizzazione, ossia l'associazione ai dati delle

[182] Cfr. DI CIOMMO F., *Diritti della personalità tra media tradizionali e avvento di Internet*, in G. Comandé (a cura di), *Persona e tutele giuridiche*, Torino, 2003, pp. 3 ss.
[183] Un motore di ricerca (in inglese "*search engine*") è un sistema automatico che analizza un insieme di dati, spesso da esso stesso raccolti, e restituisce un indice dei contenuti disponibili classificandoli in base a formule statistico-matematiche che ne indichino il grado di rilevanza data una determinata chiave di ricerca. Nel web, in particolare, i motori di ricerca sono i siti che offrono il servizio *online* di rinvenimento in tempo reale dei contenuti di *Internet*, pubblicati su altri siti, c.d. siti sorgente, che possono soddisfare le esigenze dell'utente, individuati in funzione delle parole che l'utente immette nel motore e dunque usa per svolgere la sua ricerca. Sul punto cfr. DI CIOMMO F., *Quello che il diritto non dice. Internet e oblio*, cit., p. 1101.
[184] Cfr. DELFINI F., FINOCCHIARO G., *Diritto dell'informatica*, Milano, 2014, p. 165.
[185] Cfr. Pretore di Roma, sentenza del 6 maggio 1974, cit., p. 514.

informazioni che costituiscono il contesto e che consentono di attribuire ai dati quel peso che ad essi su *Internet* spesso manca[186].

2. Il concetto di "dati personali" nella società dell'informazione.

Parlare di "protezione dei dati personali" implica, anzitutto, la necessità di procedere alla identificazione del "dato personale" – quale *species* del *genus* "dato" –, poiché solo così sarà possibile, successivamente, passare ad individuare lo strumento giuridico più idoneo per la sua protezione. Non è sufficiente, infatti, la mera proclamazione di tutela, ma è necessario, partendo proprio dalle connotazioni dell'oggetto stesso, declinare i caratteri della protezione sulle sue esigenze di tutela, al fine di garantirne l'efficacia[187].

Il punto di partenza è l'analisi del c.d. processo di "*datification*" ("datificazione") che connota strutturalmente la società contemporanea, il quale si sviluppa essenzialmente su tre piani.

Il primo piano attiene al fatto che ormai siamo dei c.d. "*walking data generators*"[188], ossia siamo in grado, a seguito dell'avvento della tecnologia – in particolare, con gli *smartphones* o, più in generale, con tutta la categoria degli strumenti c.d. "*digitized devices*" – di produrre, consapevolmente o meno, una gran quantità continua di dati, di varia specie e natura, o di utilizzare, comunque, tecnologie che sono connesse in rete deputate alla raccolta ed al trasferimento dei dati: si pensi al c.d. *Internet delle cose*[189] e alle tecnologie invasive della *privacy*, le

---

[186] Cfr. DELFINI F., FINOCCHIARO G., *Diritto dell'informatica*, cit., pp. 168 ss.

[187] Cfr. sul punto, cfr. COSTA P., *Diritti fondamentali (storia)*, in *Enciclopedia del diritto*, Annali II, Milano, 2008, pp. 365 ss.; MESSINETTI D., *Oggetto dei diritti*, in *Enciclopedia del diritto*, XXIX, Milano, 1979, pp. 808 ss.

[188] Cfr. NEWELL S., MARABELLI M., *Strategic opportunities (and challenges) of algorithmic decision-making: a call for action on the long-term societal effects of "datification"*, in *Journal of Strategic Information Systems*, 24/2015, p. 5, che riprendono l'espressione utilizzata da MCAFEE A., BRYNJOLFSSON E., *Big data: the management revolution*, in *Harvard Business Review*, n. 10, 2012, pp. 60-68.

[189] Quando si parla di Internet delle cose, o, per dirla con l'acronimo inglese IoT (*Internet of Things*) si intende fare riferimento al sistema della connessione a Internet di strumenti tecnologici diversi dai *computer*. Più nello specifico, *Internet*, infatti, è una rete globale di *computer*, cui è possibile

c.d. "*Privacy-Invading Technologies*" (PITs), cioè a tutte le forme e tipi di tecnologia, *hardware* o *software*, prodotti o servizi, che minacciano la *privacy* o possono essere usate per violare il diritto individuale alla protezione dei dati personali o alla riservatezza. Si tratta di strumenti tecnologici in grado di consentire la raccolta di una mole impressione di dati prodotti e fatti circolare da imprese, istituzioni, persone, che cresce progressivamente, *online* e *offline*[190].

Il secondo piano della datificazione riguarda, invece, la capacità di analizzare questa considerevole quantità, in costante crescita, di dati. Si tratta, a ben vedere, di un aspetto particolarmente articolato, foriero di interessanti conseguenze sulla quotidianità della vita. Orbene, fin quando tali dati rimangono in quello stato che parte della dottrina ha definito "grezzo" – c.d. "*raw data*"[191] –, essi non accrescono l'informazione e la conoscenza, posto che il dato così inteso non rappresenta altro che una consecuzione, in forma elettronica, di *bit*. Le cose cambiano, invece, nel momento in cui, mediante l'analisi e l'osservazione di quei dati, si è in grado di trarre informazioni e, quindi, di avere ulteriori conoscenze[192],

---

accedere liberamente tramite un fornitore di accesso (*Internet Service Provider*, ISP). Storicamente, ciò è avvenuto tramite *computer*, inizialmente fissi (*desktop*), successivamente portatili (*laptop*) e poi mobili (*netbook* e *tablet*). L'evoluzione attuale ha, infine, consentito di potersi connettere ad *Internet* in misura più agevole e celere mediante l'uso degli *smartphone*, concepiti in origine, solamente per telefonare. Orbene, l'IoT ha, quindi, reso possibile la connessione in *Internet* di tecnologie che inizialmente erano state pensate per l'espletamento di funzioni completamente diverse dagli elaboratori (partendo da un tostapane nel 1990). Esso, invero, comprende tutti quegli apparecchi elettronici che svolgono una particolare funzione (per esempio rilevare la temperatura ambientale) e vogliono trasmette i dati raccolti in qualche modo alla rete *Internet*. Il merito, dunque, dell'IoT è stato quello di aver reso gli oggetti intelligenti (*smart object*), con la capacità di raccogliere dati, essere controllati in remoto e sfruttare informazioni raccolte in rete. Sul punto, cfr. in particolare, PEZZOLI E., *Internet of Things, tecnologia blockchain e diritti IP*, in *Diritto Industriale*, 2020, fasc. 2, p. 113; VENIER O., *Intelligenza artificiale, blockchain e mondo IoT: l'esperienza degli operatori*, in *Diritto Industriale*, 2020, fasc. 2, p. 165.

[190] Sul punto, in particolare, cfr. FLORIDI L., *The 4th Revolution. How infosphere is reshaping human reality*, Oxford, 2014, pp. 62 ss., il quale, in particolare, osserva come "la vita umana e la realtà antropizzata (insieme ad una quota di quella non antropizzata, come ad esempio lo spazio siderale) sono ormai proiettate in un insieme gigantesco di dati".

[191] Cfr. SOFFIENTINI M., *Privacy*, Milano, 2016, pp. 768 ss. Contra, cfr. BOWKER G.C., *Data Flakes: An Afterword to "Raw Data" Is an Oxymoron, in Raw data is an oximoron*, a cura di Gitelman, Cambridge-Massachuesetts, 2013, pp. 167 ss., il quale, in particolare, mette in discussione che si possa parlare di "*raw data*".

[192] Sul punto, in particolare, cfr. BRIGHI R., *Il ruolo dei dati informatici nella costruzione della realtà*, Roma, 2016, pp. 19 ss. e 58 ss. L'Autore sottolinea la circostanza per cui la differenza tra dato e informazione non sia poi così realmente distinguibile nella realtà dell'informatica, posto che "la rappresentazione informatica di un fatto […] della realtà fisica sotto forma di bit presuppone, anche nei casi più semplici, l'individuazione dei concetti da utilizzare per esprimere la realtà rappresentata". In altre parole, dunque, il dato presupporrebbe l'esistenza di uno schema concettuale realizzato da chi ha ideato il sistema informatico e pertanto viene assunto come informazione (cioè, sin dall'origine, come interpretazione significativa di un fatto).

posto che le porzioni di questi dati, astrattamente o lontanamente riconducibili ad un soggetto, se incrociati tra loro, possono fornire informazioni circa volontà, comportamenti, attitudini e tendenze di un individuo[193].

La principale sfida del processo di datificazione, dunque, consiste proprio nel trarre conoscenza/e dai dati, ricorrendo alla c.d. "Intelligenza Artificiale" (AI), ossia alla capacità di analisi e di gestione di tali dati, posto che una quantità così vasta di *raw data* necessita forzatamente di strumenti tecnologici di analisi che, di fatto, trascendono le possibilità umane di calcolo, i quali fanno ricorso ai c.d. algoritmi (ossia alle formule matematiche), ideati e realizzati dai c.d. "*data scientists*"[194]. Di talché, l'ausilio degli elaboratori consente di analizzarli e di individuare le connessioni tra gli stessi, producendo informazioni che possono rivelarsi preziose e inedite.

Infine, occorre considerare il terzo ed ultimo stadio della datificazione, quello che più rileva in ordine all'argomento affrontato, ossia la protezione dei dati digitali nell'era informatica e digitale. Esso si identifica con il processo tecnologico mediante il quale gli elaboratori sono in grado di analizzare in modo semi-automatico – o, addirittura, automatico – gruppi particolarmente grandi e diversificati di dati. In tale processo, il passo ulteriore che si viene a compiere è quello per cui le macchine non solo trovano le informazioni richieste da chi le programma, ma sono, altresì, in grado di produrre uno stadio di conoscenza nuovo (si tratta di un aspetto della c.d. "realtà aumentata") grazie alla capacità di ottimizzare, in processi progressivi e veloci, le correlazioni fra dati ("*deep learning*")[195]. L'informatica ha, infatti, segnato una fondamentale svolta qualitativa: come sottolineato in dottrina, infatti, "l'identificazione del dato, la sua aggregazione, la sua circolazione, così come avvengono in un sistema informatico erano prima di oggi semplicemente inconcepibili"[196]. L'elaborazione automatica e

[193] Cfr. SOFFIENTINI M., *Privacy*, cit., p. 768.
[194] Benché, oggi, tuttavia, una volta avviata l'analisi sulla base di un certo algoritmo, il computer è in grado di apprendere autonomamente dalla propria "esperienza"' di analisi e, sulla base dei dati accumulati, di procedere ad elaborare ed a generare nuovi algoritmi in grado di raffinare ed ottimizzare l'analisi dei dati. Si parla, in questo caso di c.d. "apprendimento automatico", o per dirla con una formula inglese, "*machine learning*". Sul punto cfr. CALZOLAIO S., *Protezione dei dati personali (diritto pubblico)*, in *Digesto delle discipline pubblicistiche*, Milano, 2017, pp. 594 ss.
[195] Cfr. BRIGHI R., *Il ruolo dei dati informatici nella costruzione della realtà*, cit., p. 50.
[196] Cfr. FROSINI V., *Banche dati e tutela della persona*, in *Informatica, diritto e società*, Milano, 1992, pp. 187, 190.

la trasmissione simultanea, a qualunque distanza, delle operazioni compiute dall'elaboratore consentono l'accumulo dei dati in quantità enorme (pressoché illimitata), il confronto e l'aggregazione dei dati raccolti, il facile accesso e reperimento delle informazioni, l'utilizzazione di supporti e mezzi di trasmissione che agevolano la circolazione e commercializzazione dei dati.

Così facendo, dunque, tali elaboratori forniscono, al contempo, le informazioni rilevanti per chi le programma grazie alla loro capacità di analisi e di miglioramento della analisi, ma producono anche gruppi di dati nuovi, derivanti dalla correlazione che si può instaurare tra i diversi dati, che va oltre la capacità umana di elaborazione e previsione razionale. Si parla, a tal proposito, di c.d. "*data mining*"[197].

Orbene, l'intero processo si basa su degli algoritmi specificamente elaborati al fine dell'analisi e mediante le informazioni che si arriva a realizzare è possibile prendere le decisioni più adeguate; si tratta dell'"*algoritmic decision making*"[198].

Questo quadro prende il nome di "*big data*"[199], espressione utilizzata per indicare una situazione nella quale si hanno a disposizione quantità enormi di dati (*volume*) di contenuto e provenienza variegata (*variety*), alta e rapida capacità di analisi (*velocity*), cui più di recente si è aggiunto il profilo della qualità e affidabilità dei dati (*veracity*) e del loro valore (*value*)[200], indispensabili in quanto dagli stessi è possibile ricavare una c.d. "indole predittiva", nel senso che dalla loro analisi e correlazione è possibile trarre delle conseguenze fattuali di rilevante importanza[201].

---

[197] Cfr. BRIGHI R., *Il ruolo dei dati informatici nella costruzione della realtà*, cit., p. 42. L'Autore, in particolare, sottolinea che "le tecniche di *data mining* consentono l'estrazione di informazione implicita, nascosta, da dati già strutturati, per renderla disponibile e direttamente utilizzabile e l'esplorazione ed analisi su grandi quantità di dati allo scopo di scoprire pattern significativi".

[198] Cfr. STEINER C., *Automate this. How algorithms came to rule our world*, Penguin, 2012.

[199] Cfr. BUZZACCHI C., *Tecnologia e protezione dei dati personali nella società dei big data. Problemi di profilazione e di garanzia della sicurezza pubblica*, in *Sicurezza e tecnologia*, a cura di Pizzolato, Costa, Milano, 2016, pp. 69 ss.

[200] Cfr. BRIGHI R., *Il ruolo dei dati informatici nella costruzione della realtà*, cit., pp. 41 ss.; VIOLA F., *Data mining. Sottrazione, cessione e utilizzo di dati*, in *Diritto alla riservatezza e progresso tecnologico*, a cura di Fumagalli Meraviglia, Napoli, 2015, pp. 189-191.

[201] Celebre è il caso accaduto qualche anno fa nel Minnesota. Una giovane ragazza riceveva a casa alcuni buoni-sconto per prodotti usati in gravidanza da una catena di negozi statunitense (*Target*). Il padre della ragazza, infastidito dalla campagna promozionale, si recava nel punto vendita più vicino per protestare con il direttore, sottolineando che in quel modo si finiva per sollecitare la ragazza a restare incinta. Il responsabile del negozio si scusava con il padre della ragazza e, qualche tempo dopo, si premurava persino di richiamarlo a casa. Durante la conversazione, tuttavia, era il padre della ragazza a scusarsi, poiché - affermava - erano successe cose di cui non si era accorto e di lì a poco sua figlia avrebbe partorito un bimbo. Tale storia ha una portata significativa, in quanto

Orbene, la connessione tra il secondo ed il terzo piano descritti, ossia tra la capacità di analisi e la capacità di estrazione di informazioni e di prendere decisioni su tali dati, consente di trasformare anche il modo di categorizzazione dei dati personali nell'ambito della società dei dati. Invero nell'ambiente *big data* solo raramente i dati personali sono trattati in seguito ad una consapevole acquisizione del consenso dell'interessato – i c.d. "*provided data*" –; negli altri casi, di fatto, originano da trattamenti almeno secondari, in cui i dati, appunto, sono tratti dall'osservazione dell'interessato ovvero derivati o dedotti da altri dati personali. Invero, la lettura combinata di marcatori, tra cui *cookie* e altre forme di elementi tecnici, ne sono l'emblema[202]. In campo informatico, non solo applicazioni a questo deputate possono fornire dati a fronte dei quali ricostruire informazioni personali. Anche solo semplici elementi tecnici, quali i *log* di sistema, se osservati attraverso filtri socio-comportamentali, possono raggiungere lo scopo.

Da quanto sin qui descritto, dunque, può comprendersi come il concetto di dato personale sia un concetto dinamico: esso può costituire il frutto dell'analisi sviluppata dagli elaboratori e può perdere i suoi connotati caratteristici durante il processo di analisi, per poi riassumerli repentinamente[203].

Come sottolineato in dottrina, tuttavia, vi è un aspetto rilevante da sottolineare. Le macchine individuano le correlazioni fra dati secondo modalità e processi che non sempre spiegano la causa delle correlazioni osservate. Si parla, in tale evenienza, di "*black-box*"[204], espressione utilizzata per alludere alla difficoltà di decifrare il percorso logico seguito dalla macchina nel progredire nelle correlazioni fra dati[205]. Di talché, sovente si può conoscere l'esito delle analisi dei

---

dimostra come mediante l'analisi dei dati, una catena di negozi può riuscire persino, sulla base degli acquisti effettuati confrontati con un paniere selezionato di prodotti, a prevedere lo stato e lo stadio di gravidanza di una donna. Cfr. sul punto DUHIGG C., *How companies learn your secrets*, The New York Times Magazine, 16 febbraio 2012, consultabile in *http://www.nytimes.com/*.

[202] Cfr. sul punto, O'KEEFE C.M., *Privacy and Confidentiality in Service Science and Big Data Analytics*, in J. Camenisch, S. Fischer-Hubner, M. Hansen, *Privacy and Identity Management for the Future Internet in the Age of Globalization*, London, 2015, pp. 54 ss.

[203] Cfr. CALZOLAIO S., *Protezione dei dati personali (diritto pubblico)*, cit., pp. 594 ss.

[204] Cfr., sul punto, in particolare, CASTELVECCHI D., *Can we open the black-box of AI?*, in *Nature*, n. 538, 2016, consultabile in *http://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731*.

[205] Cfr. WITTEN I. H., FRANK E., HALL M., PAL C., *Data Mining. Practical Machine Learning Tools and Techniques* 4, Morgan Kaufmann-Elsevier, 2017, p. 6. In particolare, gli Autori individuano una distinzione nell'ambito dell'attività di estrazione di dati (*data mining*) nel sistema di apprendimento automatico (*machine learning*) tra la *black-box*, in cui le correlazioni fra dati non

dati operate dall'elaboratore, ma non si può dimostrare razionalmente la ragione per cui la correlazione dei dati conduce a tali risultati.

Si tratta di un aspetto, nell'ambito del processo di datificazione, complesso, ma, al contempo, anche particolarmente rilevante, poiché l'interessato, cui i dati personali analizzati si riferiscono, può essere soggetto ad una decisione, assunta da parte di un umano, fondata su quella analisi dei dati sviluppata dalla macchina. Di talché, nella società dei dati – cioè nella progressione attuale della relazione fra dati, informazioni, conoscenza, decisione e protezione dei dati personali – la parte più rilevante della tutela dei dati personali ha ad oggetto il lato oscuro della analisi dei dati, ove si realizzano correlazioni ignote fra dati, in grado di produrre informazioni incisive sulle persone o sul gruppo in cui sono collocate all'esito della analisi[206].

Invero, occorre considerare che la *datification* ha esponenzialmente aumentato la capacità di controllo (dei dati) sui soggetti, posto che l'insieme di questi dati rappresenta una miniera d'oro per lo sviluppo razionale di tutte le politiche pubbliche ipotizzabili, qualora debitamente analizzato.

2.1. (*Segue*) La commercializzazione e la protezione dei dati personali.

La moderna economia – ormai volta al digitale[207] – è sempre più "*data driven*"[208], ossia guidata e dipendente dai risultati prodotti dall'analisi di enormi

sono comprensibili e *transparent box*, in cui il procedimento di correlazione fra i dati analizzati è osservabile.

[206] Cfr. CALZOLAIO S., *Protezione dei dati personali (diritto pubblico)*, cit., pp. 594 ss.

[207] Quando si parla di economia digitale – o "*new economy*" – si fa riferimento ad un'economia sempre di più fondata sull'uso dei dispositivi tecnologici ed informatici che, in generale, comprende tutte quelle attività che si avvalgono di soluzioni digitali e che ad esse fanno riferimento. Kevin Kelly, *executive editor* della rivista *Wired*, per sottolineare il passaggio dalla c.d. *Old-economy*, o meglio dall'economia tradizionale, alla *New-economy*, afferma: "*Forget supply and demand. Forget computers. Today communication, not computation, drives change. We are rushing into a world where connectivity is everything, and where old business know-how means nothing. In this new order, success flows primarily from understanding networks, and networks have their own rules*" (Traduzione: "Dimentica la legge della domanda e dell'offerta. Dimentica i computer. Oggi la comunicazione, non i calcoli, guida il progresso. Stiamo entrando in un mondo dove la connettività è tutto, e dove le conoscenze economiche pregresse non hanno significato. In questo nuovo ordine economico, il successo deriva prima di tutto dalla conoscenza dei networks, e i networks hanno regole precise e indipendenti"). Cfr. KELLY K., *New Rules for the New Economy: 10 Radical Strategies for a Connected World*, Penguin Books, 2004, p. 7.

[208] In tema di "*data driven*", cfr. in particolare, STAZI A., CORRADO F., *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Diritto dell'Informazione e dell'Informatica*, fasc. 2, 2019, pp. 443-487. Scrivono gli Autori: "*La Data*

quantità di dati, dai quali si estraggono informazioni rilevanti per l'attività di impresa e utili al cittadino per accedere a beni e servizi innovativi. Di talché, il "dato personale" ha finito per essere una risorsa fondamentale oltreché una moneta di scambio[209]. Al dato, personale e non, infatti, ormai si riconosce un valore patrimoniale[210], con la conseguenza che il trattamento dei dati personali finisce con il passare da una dimensione "morale"– che vede nel dato un'esplicazione dell'identità e della personalità del soggetto[211] e, conseguentemente, nel diritto al corretto trattamento dei dati personali un diritto fondamentale[212] – ad una

Driven Innovation consiste sostanzialmente nell'adozione di un approccio sistematico e metodologico capace di garantire la trasformazione dei dati in innovazione. Più specificamente, il concetto fa riferimento alla capacità delle imprese e degli organismi pubblici di utilizzare le informazioni derivanti dall'analisi dei dati al fine di prendere decisioni consapevoli o di sviluppare prodotti e servizi migliori, in grado di semplificare la vita quotidiana degli individui e delle organizzazioni. In tale prospettiva, l'attività di analisi dei dati diviene un fattore chiave dello sviluppo economico e sociale".

[209] Parte della dottrina non ha esitato a qualificare l'informazione alla stregua di un "bene". In tal senso, in particolare, cfr. RODOTÀ S., *Tecnologie e diritti*, cit., pp. 52 e ss.; ZENO-ZENCOVICH V., *voce Informazione (profili civilistici)*, in *Digesto delle discipline privatistiche*, sezione civile, IX, Torino, 1993, pp. 420 e ss.; PARDOLESI R., MOTTI C., *L'informazione come bene*, in G. De Nova (a cura di), *Dalle res alla new properties*, Milano, 1991, pp. 37 ss.; RESTA G., *Autonomia privata e diritti della personalità*, Napoli, 2005, pp. 209 e ss.; GIANNONE CODIGLIONE G., *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in *Diritto dell'Informazione e dell'Informatica*, fasc. 4-5, 2015, pp. 909-938.

[210] Cfr. DE FRANCESCHI A., *Il "pagamento" mediante dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 1389. Si veda anche la sentenza del TAR Lazio, sezione I, sentenza del 10 gennaio 2020 n. 261, in *Quotidiano Giuridico*, 2020: "A fronte della tutela del dato personale quale espressione di un diritto della personalità dell'individuo, e come tale soggetto a specifiche e non rinunciabili forme di protezione, quali il diritto di revoca del consenso, di accesso, rettifica, oblio, sussiste un diverso campo di protezione del dato stesso, inteso quale possibile oggetto di una compravendita, posta in essere sia tra gli operatori del mercato che tra questi e i soggetti interessati".

[211] Cfr. RODOTÀ S., *Il diritto di avere diritti*, cit., pp. 397 ss. L'Autore, in particolare, ritiene esserci stato nel corso del tempo e a seguito dell'evoluzione tecnologica e digitale un passaggio da una concezione "statica" del diritto alla riservatezza ad una visione dinamica, legata all'enorme circolazione dei dati nell'attuale società, con l'inevitabile conseguenza che: "le persone hanno sempre di più bisogno di una tutela del loro "corpo elettronico"". In tal senso, la *privacy* – intesa in senso sociale – porta con sé la necessità di una tutela dinamica, che segue i dati nella loro circolazione.

[212] Sul punto RODOTÀ S., *Il diritto di avere diritti*, cit., p. 399. L'Autore, in particolare, individua a tal proposito un "autonomo diritto fondamentale" indispensabile per il libero sviluppo della personalità anche nelle relazioni sociali dell'individuo. Cfr., altresì, RODOTÀ S., *Tecnologie e diritti*, cit., pp. 151 e 152, nel quale l'Autore ritiene che questo possa qualificarsi come un nuovo diritto rispetto a quelli previsti esplicitamente nella Carta costituzionale. Ancora, MODUGNO F., *I "nuovi diritti" nella giurisprudenza costituzionale*, Torino, 1995, p. 123 fa rientrare il diritto alla protezione dei dati personali tra i diritti fondamentali della persona previsti all'art. 2 della Costituzione. In tal senso cfr. CALIFANO L., *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, pp. 13 ss.; CALIFANO L., *Trasparenza e privacy: la faticosa ricerca di un bilanciamento mobile*, in L. Califano, C. Colapietro (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, 2014, pp. 47 ss.; COLAPIETRO C., *I principi ispiratori del Regolamento UE*

"negoziale" (o di sfruttamento economico[213]) e di commercializzazione dei dati – che ritiene il dato suscettibile di scambi negoziali aventi rilievo economico e corrispondente a un interesse patrimoniale dei soggetti coinvolti –.

Il vantaggio di considerare questi due aspetti del dato personale, come due facce della stessa medaglia, risiede nel fatto che il soggetto nel contesto digitale, sempre più, contemporaneamente, utente, consumatore e interessato del trattamento, potrebbe beneficiare non solamente die tradizionali strumenti di tutela di un diritto fondamentale, ma anche di quelli di tipo negoziale e a tutela del consumatore, completando così il sistema di norme a "protezione" dell'utente inteso come summa di "consumatore"[214] e "interessato del trattamento"[215].

Va considerato, infatti, che sovente accade che vengano offerti dei servizi agli utenti apparentemente gratuiti[216], posto che, invece, tali servizi sono finanziati tramite la raccolta dei dati personali degli utenti reimpiegati nel mercato della pubblicità *online*. La dottrina ha coniato l'espressione di "*Internet cost trap*"[217], o, per dirla in italiano, "trappola del dono", intendendo, con tale formula il fatto che l'utente verrebbe ad essere quasi tratto in inganno: gli viene offerto un servizio apparentemente gratuito[218] e in cambio costui cede, più o meno consapevolmente,

---

2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale, in *Federalismi.it*, 22, 2018, p. 9.

[213] Cfr. BRAVO F., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018, passim.

[214] Ai sensi dell'art. 3, primo comma, lettera a), decreto legislativo n. 206 del 6 settembre 2005, Codice del Consumo: "consumatore o utente: la persona fisica che agisce per scopi estranei all'attività imprenditoriale (commerciale, artigianale) o professionale eventualmente svolta".

[215] A norma dell'art. 4, n. 1, del Regolamento UE 2016/679: "«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

[216] Cfr. RESTA G., ZENO-ZENCOVICH V., *Volontà e consenso nella fruizione dei servizi in rete*, *in Rivista trimestrale di diritto e procedura civile*, fasc. 2, 2018, p. 414. Sottolinea l'Autore, "La caratteristica di tutti questi servizi è quella di essere forniti senza la richiesta di un corrispettivo monetario. Il che ha fatto sostenere – per lungo tempo e chiudendo gli occhi alla realtà – che si trattasse di servizi "gratuiti". Nello stesso senso, cfr. STAZI A., CORRADO F., *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, cit., pp. 443 ss.

[217] Cfr. DE FRANCESCHI A., *Il «pagamento» mediante dati personali*, cit., pp. 1387 ss.

[218] In tal senso cfr. RICCIUTO V., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Diritto dell'Informazione e dell'Informatica*, fasc. 4, 2018, p. 709. L'Autore sul punto scrive: "Apparente assenza, però. In quest'ultimo caso vi è comunque, da parte dell'utente, la sopportazione di un sacrificio in funzione dell'acquisto delle applicazioni suddette".

i propri dati personali. Tale sfruttamento di dati è tanto più profittevole se preceduto da un'attività di profilazione dell'utente che permettere di realizzare la più preziosa "pubblicità mirata" o "targettizzata"[219].

Ecco perché si sono elaborate le teorie della "commercializzazione" o, anche, "monetizzazione" o "patrimonializzazione" dei dati personali[220], proprio per sottolineare la possibilità di attribuire al dato un valore economico, di scambio, tanto da poter essere accostata a quella della moneta[221]. Tali teorie si basano sull'assunto per il quale essendo i dati relativi alle persone fisiche, gli *asset* e le risorse su cui si fonda il *business* delle nuove attività d'impresa, in particolare delle piattaforme digitali, e poiché la cessione di tali dati costituisce la controprestazione dovuta dall'utente per usufruire di servizi digitali, allora questi dati sono di fatto usati come una moneta, un bene di scambio e, quindi, il servizio non sarebbe tecnicamente gratuito.

Ciò non toglie, peraltro, che possa accadere anche il contrario, ossia che siano gli utenti stessi a concedere i propri dati personali alle imprese venendo remunerati con dei servizi digitali. Invero, "posto che il valore sta nei dati, la concorrenza innovativa sta nel creare nuovi servizi che possano essere considerati un corrispettivo per la loro cessione. Non ci sarebbe dunque nulla di strano se una impresa versasse un contributo monetario (ad es. sotto forma di uno sconto sul prezzo) all'utente che le fornisce i dati"[222], con la conseguenza che dovrebbero

---

[219] Sul punto, SESSO SARTI O., *Profilazione e trattamento dei dati personali*, in L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, pp. 573-626; MONTUORI L., SIANO M., *Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione*, in G. Busia, L. Liguori, O. Pollicino, *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, 2016, pp. 101-126. Entrambi gli Autori, in particolare, individuano le problematiche giuridiche relative alla profilazione.

[220] Cfr. RESTA G., ZENO-ZENCOVICH V., *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 414: "Da un lato la storia del diritto, dai suoi albori al presente, ci offre infiniti casi in cui il corrispettivo di una prestazione non ha una natura monetaria, dalla permuta, al comodato, ai *fringe benefits*. Dall'altro la teoria economica ci fornisce tutti gli strumenti concettuali per distinguere fra attività effettivamente gratuite (tipicamente la beneficenza posta in essere da soggetti che non hanno scopi di lucro) e attività poste in essere da una impresa per finalità che non hanno un immediato ritorno monetario, ma che ne accrescono il valore (la pubblicità istituzionale, la distribuzione di campioni gratuiti, le attività benefiche)". Sul punto cfr., altresì, RICCIUTO V., *La patrimonializzazione dei dati personali*, in *Diritto dell'Informazione e dell'Informatica*, cit., pp. 689-733.

[221] Cfr. DE FRANCESCHI A., *Il "pagamento" mediante dati personali*, cit., p. 1389.

[222] Cfr. RESTA G., ZENO-ZENCOVICH V., *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 417.

essere gli interessati a dover essere retribuiti dal titolare per l'utilizzo dei loro dati[223].

Si tratta, dunque, di una concezione "proprietaria" dei dati personali in virtù della quale solo l'interessato, ossia il soggetto a cui sono riferiti i dati, ha il controllo degli stessi e può decidere chi e come può utilizzare i suoi dati e, conseguentemente, ha diritto a essere retribuito per tale utilizzo. Ciò, d'altro canto, si pone perfettamente in linea con i presupposti tradizionali della tutela dei dati personali che ravvisa nel dato un'estrinsecazione della persona[224].

A tale concezione, tuttavia, si può opporre una critica: essendo il dato personale l'estrinsecazione dell'identità e della personalità dei soggetti[225], il diritto alla protezione dei dati personali va considerato un diritto fondamentale, ossia, un diritto assoluto, indisponibile, intrasmissibile, imprescrittibile, con conseguente esclusione della possibilità di ogni commercializzazione di attributi importanti del proprio essere[226]. Ecco perché, il giurista si è spesso dimostrato riluttante nel guardare al dato personale come potenziale oggetto di una prestazione all'interno dei contratti di scambio[227].

---

[223] Interessante sul punto l'intervento di Cfr. HARARI Y.N., *21 lezioni per il XXI secolo*, Milano, 2018, p. 116, il quale rileva come: "La gara per ottenere i dati è già iniziata e vede in testa giganti high-tech come *Google*, *Facebook*, *Baidu* e *Tencent*. Finora queste aziende sembrano avere adottato il modello di *business* dei 'mercanti dell'attenzione'. Catturano la nostra attenzione fornendoci informazioni gratuite, servizi e intrattenimento, e rivendendo poi la nostra attenzione alle aziende inserzioniste".

[224] Cfr. RESTA G., ZENO-ZENCOVICH V., *Volontà e consenso nella fruizione dei servizi in rete*, cit., pp. 424 ss.

[225] Cfr. RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica di diritto privato*, 1997, p. 583.

[226] In tal senso cfr., in particolare, RICCIUTO V., *La patrimonializzazione dei dati personali*, cit., pp. 698 ss.: "Al pari degli altri attributi della persona (si pensi ai diritti sul corpo, art. 5 c.c.), non viene concepita nessuna possibilità di vendita o redditività del dato personale". In senso conforme, MESSINETTI D., *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, cit., pp. 350 ss.; DE CUPIS A., *I diritti della personalità*, Milano, 1982, p. 91; ZENO-ZENCOVICH V., *Profili negoziali degli attributi della personalità*, in *Diritto dell'Informazione e dell'Informatica*, 1993, pp. 545 ss.

[227] Sul punto ZENO-ZENCOVICH V., *Profili negoziali degli attributi della personalità*, cit., pp. 545 ss.: "la problematica della rilevanza giuridica degli attributi della personalità è stata fortemente influenzata, fin dal suo sorgere, da considerazioni etico-morali, evidenziandosi da un lato la "sacralità" della persona, dall'altro la sua non monetizzabilità. Ne sono eloquente conferma il travaglio di dottrina e giurisprudenza in ordine al risarcimento del danno non patrimoniale; e, specularmente, la refrattarietà, solo di recente sovvertita, ad attribuire valore economico alle lesioni della personalità. In questo contesto non stupisce che si siano ritenute le categorie del negozio giuridico e dei diritti della personalità se non antitetiche almeno scarsamente comunicanti fra loro".

Tale lettura si pone, peraltro, in linea con la collocazione sistematica del diritto alla protezione dei dati personali all'interno del sistema di tutela della riservatezza e tra i diritti fondamentali della persona[228], come disposto dagli articoli 8 della Convenzione Europea dei Diritti dell'Uomo, 8 della Carta dei diritti fondamentali dell'Unione europea, nonché 16 del Trattato sul Funzionamento dell'Unione europea[229].

Tuttavia, benché quanto detto può essere accolto, vi è da considerare che, nella pratica, sovente, il dato personale viene scambiato per beni e servizi. Sebbene, infatti, la "trappola del dono" sia un fenomeno ormai conosciuto, il cittadino o l'utente non sembrerebbe curarsene. Ciò potrebbe, senz'altro, essere conseguenza della forte asimmetria informativa implicita ai servizi digitali che, oltre a essere giuridica e/o economica è spesso anche e soprattutto tecnica. Ma potrebbe, altresì, essere conseguenza di una libera scelta dell'utente che consapevolmente cede i propri dati per accedere ad un servizio che altrimenti non potrebbe permettersi.

Non può, dunque, porsi in dubbio il fatto che la commercializzazione dei dati sia ormai una realtà. Ma, a ciò occorre necessariamente aggiungersi anche la constatazione per cui, è vero che i dati personali sono oggetto di cessione, ma è anche vero che questi non sono *sic et simpliciter* informazioni commerciali, bensì attengono strettamente alla personalità umana e contribuiscono a disegnarne la personalità, l'identità e, non ultimo, la dignità[230].

---

[228] RICCIUTO V., *La patrimonializzazione dei dati personali*, cit., p. 697.

[229] Importante sul punto è anche l'intervento del Garante per la Protezione dei Dati Personali che, nell'ambito della relazione annuale per l'anno 2018, ha parlato di "dividendo dei dati". Secondo il Presidente Antonello Soro: "Il diritto alla protezione dei dati personali viene sempre più invocato di fronte alle innumerevoli 'servitù volontarie' cui rischiamo di consegnare noi stessi, in cambio di utilità e servizi che paghiamo al prezzo di porzioni piccole o grandi della nostra libertà. Emerge così un nuovo sottoproletariato del digitale, un 'Quinto Stato' formato da quanti siano disposti a cedere, con i propri dati, la libertà, in cambio dei servizi offerti in rete solo apparentemente 'a prezzo zero'". Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Relazione annuale per il 2018*. Discorso del Presidente Antonello Soro, Roma, 7 maggio 2019.
Negli stessi termini si era già anche espresso il Garante europeo, l'*European Data Protection Supervisor* che, nel suo parere del marzo 2017, con riferimento alla possibilità di equiparare i servizi generalmente considerati "gratuiti", ma in realtà pagati con lo scambio di dati personali, a quelli "a pagamento" tradizionali, ha affermato: "*The EDPS welcomes the intention of the legislator to make sure that the so-called "free services" are subject to same protection for the consumers when they do not pay a price for a service or content. However, personal data cannot be compared to a price, or money. Personal information is related to a fundamental right and cannot be considered as a commodity*". Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017.

[230] Cfr. D'IPPOLITO G., *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Diritto dell'Informazione e dell'Informatica*, fasc. 3, 2020, p. 634.

Ferma restando la rilevanza costituzionale del diritto alla protezione dei dati personali, dunque, il punto di equilibro potrà rintracciarsi nel tentativo di non far prevalere la logica economica su quella della tutela dei diritti umani, ma di affiancare all'approccio morale quello negoziale, riconciliando i due aspetti rilevanti dello stesso fenomeno e completando il sistema delle tutele per l'interessato che è certamente un consumatore o utente ma, prima di tutto, è una persona, il cittadino della nuova realtà c.d. "*on life*"[231] e nuovo "soggetto debole" meritevole di ulteriore protezione [232].

3. L'origine del concetto di "*Privacy*".

Dopo aver individuato le problematiche principali inerenti la tutela dell'identità personale dell'individuo in rete e quelle riguardanti la protezione dei dati personali nell'era digitale, passiamo ora a vedere quale sia stato lo sviluppo della normativa italiana in merito alla tematica della tutela della *privacy* – fino al Regolamento Europeo del 2016, oggetto di trattazione del prossimo capitolo, con specifico riferimento alla *blockchain* –, per comprendere quale sia la regolamentazione sostanzialmente applicabile.

La prima considerazione da cui partire è che, generalmente, i diritti sono sempre figli del proprio tempo, della società in cui nascono e si sviluppano. Alcuni tra di essi, tuttavia, finiscono con l'essere maggiormente legati, rispetto ad altri, all'epoca nella quale hanno fondato le proprie radici. Ed è così che le istanze che si vengono a porre finiscono per diventarne uno specchio fedele dal quale è possibile ricavare l'immagine stessa della società che, dapprima, ne ha avvertito il bisogno,

[231] Espressione coniata da FLORIDI L., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, p. 17, per evidenziare la natura ibrida della nostra vita, in parte digitale e in parte analogica. In tal senso, cfr., altresì MORELLI A., *I diritti e la Rete. Notazioni sulla bozza di Dichiarazione dei diritti in Internet*, in *Federalismi.it*, fasc. 1, 2015, pp. 3 ss.

[232] Cfr. D'IPPOLITO G., DI MARTINO G., DOLMETTA M.C., *Evoluzione della disciplina consumeristica e rapporto con la normativa sulla protezione dei dati personali*, in *Consumers' Forum*, *Consumerism 2019. Dal codice del consumo al Digital Service Act. Quella dal consumatore al cittadino digitale è vera evoluzione?*, 2019, pp. 70-81.

quindi, reclamato la tutela, ed, infine, forgiato le forme. Tra questi, vi è sicuramente il diritto alla "*privacy*"[233].

Nella sua ormai lunga evoluzione, esso ha accompagnato gli sviluppi della nostra società, seguendone le mutevoli esigenze ed adattandosi ad esse. Nel secolo scorso, di fronte ai fenomeni di crescente concentrazione della popolazione nelle città, la domanda di riservatezza era soprattutto una richiesta di protezione dalle indebite intrusioni dei vicini in ciò che accadeva all'interno delle mura domestiche. È proprio questo il contesto della tranquilla Boston di fine Ottocento, dove ormai tradizionalmente si tende ad individuare la nascita del diritto alla *privacy*[234]. In particolare, si rammenta un episodio decisivo per la nascita di questo diritto, ossia quello avvenuto nella piccola comunità nella quale l'avvocato *Samuel Warren*, stanco di leggere sulla Gazzetta locale delle attività mondane della moglie e delle relazioni della figlia, decise di scrivere col suo amico *Louis Brandeis*, allora professore ad Harvard, un saggio dedicato proprio al *Right to Privacy*. Si apriva, così, la strada al riconoscimento di un diritto destinato ad incidere ben al di là delle vicende personali della famiglia Warren[235].

Nell'ordinamento statunitense, infatti, partendo da tale premessa, la nozione di "diritto alla *privacy*" è stata elaborata per la prima volta intorno alla metà del XIX secolo[236] ed ha mantenuto inalterata la sua denominazione anche negli altri

---

[233] Cfr. BUSIA G., *voce Riservatezza (diritto alla)*, in *Digesto delle discipline pubblicistiche*, IV agg., Torino, 2000, pp. 476-510.

[234] Sul punto, in particolare, cfr. RODOTÀ S., *Tecnologie e diritti*, cit.. L'individuazione di un momento specifico nel quale il diritto sarebbe nato assume un valore meramente simbolico e convenzionale, ragion per cui vi è anche chi riconduce la sua origine ad altri episodi. Così, ad esempio, è possibile individuarne l'origine nel *case Prince Albert v Strange* del 1849 (1 Mac and G 25, 1 H e TW1, *Court of Chancery*). Alla base della pronuncia, uno scontro fra la regina Vittoria ed il principe Alberto, che avevano fatto eseguire alcune acqueforti raffiguranti i loro figli, ed un dipendente della casa reale, che aveva effettuato copie abusive dei quadri al fine di pubblicarle all'interno di un catalogo. Il *Lord Chancelor* diede ragione ai regnanti non solo per la violazione al diritto di proprietà dell'autore delle opere, ma anche - ed è questo il punto che qui interessa - per il mancato rispetto della tacita intesa di riservatezza che deve presumersi intercorrere fra il dipendente ed i suoi datori di lavoro. Anche questo atto di nascita del diritto alla *privacy* trova però proprio al suo interno un ulteriore spunto per risalire ancora più indietro, a conferma del valore puramente simbolico di questi riferimenti. Nella stessa pronuncia si trova infatti un richiamo ad un precedente (*Tipping v. Clarke*, 2 Hare, 393), in base al quale ogni dipendente di una casa privata assume contrattualmente un implicito obbligo di riserbo. Cfr., CERRI A., *Riservatezza (diritto alla)*, II, *Diritto comparato e straniero*, in *Enciclopedia giuridica*, XXVII, Roma, 1991, par. 2.1.

[235] Cfr. WARREN S., BRANDEIS L.D., *«The Right to Privacy»*, *Harvard Law Review*, fasc. 4, 1890, pp. 193 ss.

[236] Cfr. PARDOLESI R., *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, pp. 3 ss.

Stati democratici, malgrado abbia stentato ad attecchire. La ricostruzione più recente del concetto di *privacy* è avvenuta ad opera di un recente intervento della Corte Suprema Americana[237], la quale ha individuato vari settori della vita dei singoli che necessitano di una più accurata garanzia di riservatezza, in assenza della quale il sistema delle libertà personali non potrebbe essere sufficientemente garantito. Nel suo ragionamento, spesso la Corte, facendo riferimento al I emendamento della Costituzione Americana, il quale riconosce una serie di libertà ai cittadini, ricomprende tra di essi anche il diritto alla riservatezza, identificabile proprio come principio di libertà individuale.

Per quanto, invece, attiene all'evoluzione del diritto alla *privacy* negli ordinamenti Europei, il riferimento storico è, senza dubbio, il periodo successivo alla seconda guerra mondiale durante il quale comincia a diffondersi l'interesse per l'individuazione di una specifica tutela al valore della riservatezza, mediante l'attuazione di disposizioni in grado di fissare adeguati principi e regolamenti. Sintomatico di questa nuova tendenza è senz'altro l'ordinamento tedesco[238], nel quale venne, già all'epoca, emanata un'importante normativa che forniva una disciplina inerente alla tutela della riservatezza come diritto del cittadino alla difesa della propria sfera privata, limitabile solo dinanzi ad un interesse pubblico di pari valenza giuridica.

Orbene, le possibilità offerte dalle nuove tecnologie dell'informazione e della comunicazione hanno via via consentito a chi detiene il potere e dispone degli strumenti tecnici e giuridici di penetrare nella sfera privata dell'individuo, anche a sua insaputa, per raccogliere determinate informazioni personali; può, inoltre, ricostruire, attraverso l'aggregazione di dati che, singolarmente considerati, hanno un significato limitato, profili individuali e di gruppo. In tal modo può esercitare il controllo sugli individui dei quali è possibile conoscere la storia personale e, sulla base di questa, prevederne ed orientarne i comportamenti futuri, anche attraverso forme di discriminazione e di esclusione verso coloro che non si conformano ai modelli prevalenti[239].

---

[237] Cfr. SIMONATI A, *L'accesso amministrativo e la tutela della riservatezza*, cit., pp. 42 ss.
[238] SIMONATI A., *L'accesso amministrativo e la tutela della riservatezza*, Trento, 2002, pp. 48 e 49.
[239] Cfr. sul punto, RODOTÀ S., *Tecnologie e diritti*, cit., p. 116. L'Autore, in particolare, sottolinea come "privilegiandosi i comportamenti 'conformi' ai profili prevalenti, si rende più difficile la

Di fronte a questo quadro è emersa la pressante esigenza di una più forte tutela della sfera intima della persona, del complesso cioè di informazioni su azioni, comportamenti, opinioni, preferenze che definiscono il nucleo della personalità individuale, e attraverso questa, in definitiva, di tutela della libertà personale, tutela cioè "delle scelte di vita contro ogni forma di controllo pubblico e di stigmatizzazione sociale"[240].

Tale protezione si è ritenuto possa realizzarsi attraverso il riconoscimento di un diritto del singolo di mantenere il controllo sull'uso delle informazioni personali che lo riguardano. Questo diritto, definito anche come "libertà informatica"[241], viene inteso come la nuova connotazione assunta, nei confronti delle moderne tecnologie dell'informazione, nell'attuale contesto sociale, dal diritto alla riservatezza (*privacy*), la situazione giuridica soggettiva nata come strumento per la protezione di spazi di libertà dell'individuo dalle altrui ingerenze.

Venendo, dunque, man mano a mutare il contesto storico, di conseguenza, anche il diritto alla riservatezza è venuto ad assumere connotazioni caratteriali piuttosto differenti rispetto a quelle che lo caratterizzavano al momento della sua nascita. Invero, in un'epoca, quale quella attuale, in cui le tecnologie dell'informazione schiudono ogni giorno nuovi orizzonti ed un numero crescente di attività implica la creazione di flussi comunicativi, i confini di tale diritto tendono ad ampliarsi trasformandone, contemporaneamente, il contenuto[242].

Alla tradizionale dimensione "negativa" di potere di esclusione dalla conoscenza e dalla divulgazione di certe informazioni personali, che aveva caratterizzato il significato del *right to privacy* alla sua nascita, alla fine del secolo scorso, dunque, se ne viene ad affiancare un'altra "positiva". Si tratta del potere di tenere sotto controllo i propri dati che siano stati già raccolti da altri soggetti,

---

produzione di nuove identità collettive, con rischi per la dinamica sociale e per la stessa organizzazione democratica".

[240] Cfr. RODOTÀ S., *Tecnologie e diritti*, cit., p. 102.

[241] Sul punto, cfr., FROSINI V., *Banche dati e tutela della persona*, cit., p. 179. In particolare, l'Autore, richiamando l'istituto dell'*habeas corpus*, utilizza anche il concetto di "*habeas data*"; come "riconoscimento del diritto del cittadino di disporre dei propri dati personali così come egli ha il diritto di disporre liberamente del proprio corpo". Invece, secondo TRAVERSI A., *Il diritto dell'informatica*, Milano, 1985, pp. 78 ss., l'espressione "libertà informatica" dovrebbe utilizzarsi nel significato di libertà di raccolta ed elaborazione dei dati.

[242] Cfr. BUSIA G., *voce Riservatezza (diritto alla)*, in *Digesto delle discipline pubblicistiche*, cit., pp. 476-510.

pubblici o privati, ed eventualmente di intervenire per integrarli, modificarli, ottenerne la distruzione. È quello che la Corte costituzionale tedesca[243] ha definito come "diritto all'autodeterminazione informativa", diritto di decidere da sé della cessione e dell'uso dei propri dati, riconoscendolo come diritto fondamentale della persona.

Di talché, il concetto di tutela della *privacy* non può più risolversi nella semplice e mera tutela contro la divulgazione di informazioni personali da parte di terzi. Il fatto che, come abbiamo visto, ogni giorno milioni di dati vengano raccolti, ordinati, elaborati, trasmessi ed anche diffusi con grandissima velocità in ogni angolo del pianeta implica la necessità di un'adeguata tutela, non solo per i soggetti che compiono le più diverse operazioni su di essi, ma anche per coloro a cui i dati si riferiscono. Anche attraverso l'uso dei dati da parte di terzi, infatti, ognuno può ottenere i servizi e i beni di cui ha bisogno nonché, più in generale, interagire con la comunità in cui vive.

Invero, in una società che si fa più ricca e complessa le relazioni si basano sempre meno sul contatto diretto con gli altri e sempre più su rapporti costruiti attraverso la comunicazione e lo scambio di informazioni personali. I dati personali – in via generale classificabili in quanto comuni, sensibili e super-sensibili[244] – sono elementi che da informazioni riservate e di difficile reperimento si sono tramutati in informazioni conoscibili e facilmente rintracciabili[245].

Di talché, l'immagine e l'identità sociale di ogni individuo si viene ad identificare sempre meno con quella, fisica e reale e, sempre di più, come abbiamo visto, con quella virtuale, frantumata nelle singole informazioni personali e volta a volta ricostruita in modo differente, a seconda dei diversi contesti in cui queste giungono e sono rielaborate nel perseguimento delle più svariate finalità.

Lo sviluppo tecnologico frequentemente viene utilizzato proprio per sottrarsi alla continua esposizione delle proprie azioni alla collettività: si pensi alle

[243] Cfr. Corte Costituzionale tedesca, sentenza del 15 dicembre 1983, *Volkszählungurteil*.
[244] Cfr. CORONA F., *La nuova dimensione della privacy con l'avvento del progresso tecnologico*, Cesena, 2014, pp. 25 ss.; FALZONE E., *Privacy in azienda*, Milano, 2007, pp. 8 ss.
[245] Cfr. SASSANO F., *Il diritto all'oblio tra internet e mass media*, Vicalvi 2015, pp. 70 ss.; VAN LIESHOUT M., *The Value of Personal Data,* in J. Camenisch, S. Fischer-Hubner, M. Hansen, *Privacy and Identity Management for the Future Internet in the Age of Globalization*, London, 2015, pp. 26 ss.

sempre più numerose attività che è possibile svolgere senza uscire dalla propria abitazione. Esso stesso, dunque, funziona come garanzia di riservatezza intesa in senso tradizionale, come freno all'invadenza di vicini troppo curiosi. Tuttavia, gli stessi mezzi che apparentemente proteggono dal controllo altrui, sono spesso in grado di registrare e catalogare tutte le azioni compiute, atteso che rendono molto più semplice sorvegliare silenziosamente la vita altrui. Generalmente, quanto più i servizi di cui ci si avvale sono sofisticati, tanto più sono capaci di conservare la memoria su quanto è stato fatto, e quindi di creare possibilità sempre nuove e forme più penetranti di intrusione nella vita privata. Non è, dunque, un caso se lo studio e la produzione normativa sulla tutela dei dati personali hanno avuto un grande sviluppo nell'ultimo trentennio, soprattutto in risposta ai progressi tecnologici nel campo dell'elaborazione elettronica dei dati (anche personali), ed alle conseguenti possibilità di ingerirsi, attraverso tali mezzi, in modo quantitativamente e qualitativamente più penetrante nella vita privata degli individui[246].

Tutto ciò, peraltro, può verificarsi senza che l'interessato possa rendersene conto – si pensi solo ai numerosi collegamenti fra le diverse banche dati, capaci di connettere i diversi dati riguardanti una stessa persona e di ricostruirne il profilo – e, spesso, senza che le legislazioni degli Stati siano in grado di tenere il passo con tale incessante evoluzione.

È sulla base di queste considerazioni che si viene a porre, dunque, il problema della protezione dei dati personali, un problema attinente proprio alla "sovranità di sé", rispetto al novero indeterminato dei soggetti pubblici e privati con cui si entra inevitabilmente in contatto e che potrebbero, in qualche modo, conoscere la portata di quanto racchiuso in tali dati. Invero, la disciplina della protezione dei dati delinea il modo con cui l'ordinamento giuridico intende garantire alla persona non solo il dominio sui dati che la identificano e, di conseguenza, la discriminano dagli altri, ma anche il libero sviluppo della sua personalità nella società dei dati, cioè nel rapporto con tutti gli altri soggetti che esercitano un potere sui dati e, su quella base, con tutti gli altri consociati[247].

---

[246] Anche in ragione di questo legame storico, molto spesso si tende a trattare del diritto alla riservatezza con riferimento all'ambito informatico quasi esclusivamente. Sul punto cfr. FRANCESCHELLI V. (a cura di), *La tutela della privacy informatica*, Milano, 1988, p. 20 ss.
[247] Cfr. CALZOLAIO S., *Protezione dei dati personali (diritto pubblico)*, cit., pp. 594 ss.

Invero, il variegato novero di soggetti che detengono il potere sui dati è in grado di esercitare un potere reale sulla persona e sulla collettività, con l'inevitabile conseguenza per cui l'avvento della società dei dati comporta concettualmente la fine del dualismo fra "spazio" e "*cyberspazio*", fra "identità personale" e "identità virtuale (o elettronica)", fra vita "*online*" e "*offline*", e, quindi, più genericamente fra mondo virtuale e reale[248].

3.1. (*Segue*) Il contributo della dottrina nazionale sull'individuazione del concetto di "*privacy*".

Nell'ordinamento nazionale, il diritto alla riservatezza e il suo inserimento nell'ambito dei diritti fondamentali della persona umana ha cominciato a suscitare l'interesse di dottrina e giurisprudenza sul finire dell'Ottocento, ossia in un momento storico di grandi mutamenti politici, economici e sociali. Giova ricordare, infatti, che il fenomeno dell'industrializzazione e tutta l'evoluzione sociale e politica che da esso ne è derivata – al pari di quanto avvenuto negli altri ordinamenti europei –, hanno mutato radicalmente lo stile di vita della collettività, favorendo l'urbanizzazione e stimolando la ricerca tecnologica.

A fronte della mancanza di un sistema di regole che disciplinasse in maniera omogenea tale istituto, la dottrina ha cominciato ad innescare varie dispute, tutte pressoché accomunate dalla medesima esigenza di fondo, ossia quella di garantire un'adeguata tutela al patrimonio giuridico individuale, in maniera tale da prevenire eventuali invasioni o interferenze di natura illegittima da parte di soggetti terzi nell'ambito delle proprie informazioni personali.

Sono state, così, individuate tre fasi, tra loro correlate, che hanno riguardato il percorso evolutivo del diritto alla riservatezza: anzitutto, la progressiva affermazione della sua esistenza giuridica; in secondo luogo, l'emersione come

[248] Particolarmente critici su questo punto, KARABOGA M.,MATZNER T., OBERSTELLER H., OCHS C., *Is There a Right to Offline Alternatives in a Digital World?*, in *Data Protection and Privacy: (In)visibilities and Infrastructures*, a cura di Leenes, van Brakel, Gutwirth, De Hert, Springer, 2017, pp. 31 ss., i quali si chiedono nello specifico se oggi possa parlarsi ed individuarsi un vero e proprio "diritto a vivere sconnessi" da parte degli individui.

nuova esigenza di tutela della personalità ed, infine, la sua "codificazione" a seguito dei vari interventi legislativi[249].

Per quanto attiene al profilo dell'esistenza giuridica di un diritto alla riservatezza, si può partire da una data ben precisa, ossia il 1937, anno nel quale viene pubblicato il lavoro di Santamaria Ferrara, intitolato "Il diritto all'illesa intimità privata", nel quale l'Autore, in particolare, racconta dell'esistenza giuridica di "un diritto, assoluto e inviolabile, della personalità, consistente nella libera facoltà di mantenere nel riserbo della intimità privata […] certi modi di essere della propria persona e certe cose o situazioni ad essa inerenti"[250].

Queste affermazioni, tuttavia, non sono state condivise da quella parte della dottrina, che ha negato, a lungo, la sussistenza di un vero e proprio diritto alla riservatezza sul presupposto che non potesse riconoscersi alcuna forma di tutela a determinati fatti personali che secondo quanto previsto dalla Costituzione non erano assoggettati all'obbligo generale di segretezza[251].

L'esigenza di fondo che ha spinto verso la richiesta di tutela è stata quella di consentire al soggetto la possibilità di estraniarsi, di "avere diritto" alla propria solitudine, di non subire ingerenze nella propria intimità[252]; e se è vera l'esistenza di una certa relatività di fondo in tema di intimità ed ingerenza – atteso che ogni individuo le avverte diversamente in quanto esse sono "quanto di più variabile si possa immaginare, avuto riguardo alla varietà ed alla complessità della propria esistenza, al proprio carattere, al ruolo sociale e così via"[253] – al contempo è anche vera l'esigenza "biologica dell'uomo alla fruizione di periodi di isolamento, materiale e psicologico"[254], pur atteggiandosi diversamente a seconda dei contesti. Il punto focale della questione è stato, invero, il riconoscimento in capo al soggetto

[249] Cfr. SCAGLIARINI S., *La riservatezza e i suoi limiti, sul bilanciamento di un diritto preso troppo sul serio*, Roma, 2013, pp. 41 ss.
[250] Passo citato da SCAGLIARINI S., *La riservatezza e i suoi limiti, sul bilanciamento di un diritto preso troppo sul serio*, cit., p.43
[251] Cfr. FOIS S., CHIOLA C., ESPOSITO C., *Sulla libertà di manifestazione del pensiero,* in SCAGLIARINI S., *La riservatezza e i suoi limiti, sul bilanciamento di un diritto preso troppo sul serio*, Roma, 2013, p. 44
[252] Cfr. FURFARO S., *voce Riservatezza*, in *Digesto discipline penalistiche*, Agg. II, Torino, 2008, pp. 1063 ss.
[253] Cfr. FIORE C., *Riservatezza (diritto alla)*, in *Enciclopedia giuridica*, Agg., XXVII, Roma, 1998, p. 3.
[254] Cfr. FURFARO S., *voce Riservatezza*, cit., pp. 1063 ss.

di non rendere noti aspetti della propria sfera privata sui quali intendeva mantenere il proprio riserbo[255].

Determinante verso il riconoscimento del diritto alla riservatezza è stato poi il contributo di una parte della dottrina privatistica che ha proceduto all'enucleazione di un diritto all'"identità personale", rilevante in quanto con esso ha cominciato a porsi la necessità di tutelare non solamente gli aspetti distintivi dell'individuo singolarmente inteso, bensì la persona umana complessivamente considerata[256].

Su tali basi, la riservatezza come diritto si è evoluta all'interno dell'ampia categoria dei "diritti della personalità", nella quale, almeno fino ai primi anni del Novecento, sono state comprese diverse posizioni soggettive della vita umana che, nonostante avessero poco in comune, sollecitavano comunque il riconoscimento e la predisposizione di adeguate tutele. Sono nati, così, quei diritti successivamente qualificati di "*first generation*", corrispondenti alle c.d. libertà civili, ossia il diritto alla vita, all'integrità fisica, alla libertà, alla proprietà privata, alle libertà di espressione, pensiero, religione e associazione e via dicendo[257].

Fondamentali sono state anche le intuizioni di Ravà, il quale, partendo dal concetto di personalità giuridica e relazionandola alla capacità di volere, è arrivato a definire il concetto di "personalità giuridica come diritto sulla propria persona", constatando l'assenza, nell'ordinamento, dell'esplicito riconoscimento di un diritto alla riservatezza, autonomo e rilevante in quanto tale. Tuttavia, egli ha, altresì, constatato come all'interno dell'ordinamento fosse comunque possibile rinvenire delle norme atte ad essere considerate manifestazione di tale diritto. Di conseguenza, egli ha ritenuto che, partendo da esse, per via analogica e facendo

---

[255] Cfr. MARTINOTTI G., *La difesa della privacy*, in *Politica del Diritto*, 1972, pp. 59 ss.

[256] Tra l'altro, l'ingresso del diritto all'identità personale nell'ordinamento giuridico trova risalto anche nella previsione di una più generale tutela dell'immagine della persona umana, menzionata dall'art. 10 Cod. Civ., malgrado essa costituisca probabilmente la lesione meno grave di un diritto alla riservatezza. Sul punto cfr. DE CUPIS A., *Il diritto all'identità personale,* in SCAGLIARINI S., *La riservatezza e i suoi limiti, sul bilanciamento di un diritto preso troppo sul serio*, Roma, 2013, p.46 ss. Questo Autore, in particolare, ha ricondotto la tutela giuridica dell'istituto della riservatezza ai valori della dignità personale e dell'onorabilità, i quali sono specificamente protetti dalla disciplina contenuta nelle disposizioni primarie, tra le quali, rientra anche la difesa del diritto al nome, a norma dell'art. 6 Cod. Civ.

[257] La dottrina sul punto ha fornito importanti contributi. Cfr., tra gli altri, ARCUDI G., POLI V., *Il diritto alla riservatezza*, Milano, 2000, p. 12; BALDASSARRE A., *Diritti inviolabili*, in *Enciclopedia giuridica*, XI, Roma, 1989, pp. 10 ss.; MESSINETTI D., *Personalità (diritti della)*, in *Enciclopedia del diritto*, XXXIII, Milano, 1983, p. 355.

riferimento ai principi generali dell'ordinamento, si sarebbe potuti pervenire ad individuare l'essenza del diritto alla riservatezza[258]. Saranno gli studi successivi del medesimo Autore, seguito, poi, anche da Carnelutti[259], che lo porteranno a definire concettualmente il diritto alla riservatezza, sulla base della constatazione per cui: "la qualità di persona richiede ed esige che alla persona stessa sia riservata una certa sfera relativa ai dati più gelosi e più intimi di essa e della sua attività"[260].

Altro oggetto di disputa è stata la natura pluralista o monista del diritto in oggetto. Alcuni Autori hanno, infatti, ritenuto che la riservatezza fosse da considerare un'entità polivalente e che non potesse, cioè, ridursi alla semplice esigenza di segretezza rispetto ad alcune ingerenze della sfera privata della persona: al contrario, risulterebbe necessario individuare in essa una portata più ampia, riconducibile, in generale, al meccanismo di circolazione e di comunicazione dei dati personali[261]. Di talché, la riservatezza verrebbe ad essere concepita come il diritto inerente a "quelle informazioni riguardanti la vita privata delle persone fisiche, dalla cui divulgazione possa derivare una lesione alla dignità della persona tale da impedirne il pieno sviluppo e l'effettiva partecipazione alla vita della comunità di appartenenza"[262].

A tale concezione pluralistica, si è, tuttavia, contrapposta una concezione monistica, prospettata dal giurista Giorgio Giampiccolo, il quale ha delineato un diritto unico alla riservatezza sul presupposto che l'individuo potesse essere qualificato alla stregua di un valore unitario; un diritto, secondo il giurista, che "non si identifica con la somma delle molteplici sue esplicazioni singolarmente protette da norme particolari"[263].

---

[258] Cfr. RAVÀ A., *Istituzioni di diritto privato*, Padova, 1938, pp. 174 e 175. In particolare, le norme richiamate dal giurista sono gli artt. 10 del Codice Civile del 1942 e gli articoli 96 e 97 della legge sul Diritto d'Autore del 22 aprile 1941, n. 633. In campo penale hanno rilevanza gli articoli da 616 a 623 del Codice Rocco.

[259] Sul punto, cfr. CARNELUTTI F., *Diritto alla vita privata*, in *Rivista Trimestrale di Diritto Penale*, Milano, 1955, pp. 3 ss.

[260] Cfr. RAVÀ A., *Istituzioni di diritto privato*, cit., pp. 174 e 175.

[261] Cfr. DE CUPIS A., *In tema di offesa morale per mezzo della divulgazione cinematografica*, in *Foro italiano*, 1949, fasc. 1, pp. 506 ss.

[262] Cfr. ARENA G., (voce) *Trasparenza amministrativa*, in *Enciclopedia Giuridica Treccani*, vol. XXXI, Roma, 1995, p .9.

[263] Cfr. PROSPERI M., *Il dibattito italiano sull'esistenza e sul fondamento del diritto alla riservatezza prima del suo espresso riconoscimento*, in *www.privacy.it.*

3.2. (*Segue*) Il contributo della giurisprudenza nazionale sul concetto di *privacy*.

Alla complessità delle diverse posizioni dottrinali che hanno cercato di individuare progressivamente l'esistenza di un fondamento giuridico del diritto alla riservatezza, ha fatto seguito il contributo della giurisprudenza.

Le prime pronunce giurisprudenziali in materia risalgono agli anni '50[264]. Nello specifico, è il 1956 l'anno in cui viene emessa la prima importante sentenza della Corte di Cassazione, a definizione della vicenda del tenore Enrico Caruso, i cui eredi, avendo ritenuto leso il proprio diritto di riservatezza da un'opera cinematografica, invocano tale lesione dinanzi ai giudici. In questo primo caso giudiziario, la presa di posizione della Corte si è orientata nel senso di negare decisamente l'esistenza giuridica del diritto alla riservatezza, affermando che "nessuna disposizione di legge autorizza a ritenere che sia stato sancito come principio generale il rispetto dell'intimità privata e tanto meno come limite alla libertà dell'arte", cosicché "l'aspirazione alla privatezza non riceve protezione salvo che l'operato dell'agente abbia leso onore o reputazione rientrando nell'illecito". Anzi, "chi non ha voluto o saputo tenere celati i fatti della propria vita non può pretendere che il segreto sia mantenuto dalla discrezione altrui, dato che curiosità e pettegolezzo, se non sono manifestazione elevata dell'animo umano, non danno luogo di per sé a illecito giuridico"[265].

Dopo questa prima presa di posizione, la Cassazione è tornata a pronunciarsi nel 1963[266]. In questa occasione, sebbene non sia ancora stato riconosciuto appieno il valore giuridico della riservatezza, la Corte, tuttavia, vi attribuisce piena tutela affermando così l'esistenza di un diritto assoluto della personalità quale diritto alla libertà di autodeterminazione di chiunque. Da tale costruzione giuridica, è derivato poi il divieto di divulgare notizie non autorizzate e attinenti alla vita privata

[264] Sul punto cfr. SCAGLIARINI S., *La riservatezza e i suoi limiti, sul bilanciamento di un diritto preso troppo sul serio*, cit., pp. 51 ss.
[265] Cfr. Corte di Cassazione Civile, sezione I, sentenza del 22 dicembre 1956, n.4487, in *Giustizia civile*, 1957, I, pp. 7 ss.
[266] Cfr. Corte di Cassazione Civile, sentenza del 20 aprile 1963 n. 990, in *Foro Italiano*, 1963, fasc. I, p. 887.

dell'individuo anche nella circostanza in cui non sussistesse un preminente interesse pubblico alla conoscenza[267].

Orbene, la successiva tappa dell'*iter* evolutivo della giurisprudenza di legittimità è rappresentata dalla sentenza n. 2129 del 1975[268], nella quale la Corte ha sottolineato l'esistenza di un duplice fondamento costituzionale dell'istituto, ravvisabile non soltanto nella legislazione ordinaria – in armonia con i principi costituzionali – ma anche nella legislazione comunitaria ed internazionale. La pronuncia del 1975 merita particolare considerazione in quanto la Cassazione finalmente afferma che "l'ordinamento giuridico riconosce e tutela l'interesse di ciascuno a che non siano resi noti fatti o avvenimenti di carattere riservato senza il suo consenso". Quindi, un diritto a che non siano resi pubblici fatti o notizie riservate senza il consenso dell'interessato.

A ben vedere, dunque, tra la prima e l'ultima rilevante decisione della Suprema Corte in materia, si assiste ad un vero e proprio coinvolgimento sulla questione dell'esistenza di un autonomo diritto alla riservatezza, il quale ha acquisito nel corso del tempo una propria rilevanza costituzionale.

3.3. (*Segue*) Le fonti in ambito comunitario in tema di riservatezza.

In ambito comunitario, le prime fonti normative che hanno riconosciuto espressamente un diritto alla *privacy* sono la Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950 (CEDU) e la Convenzione di Strasburgo del 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati personali. Proprio l'esigenza di garantire il diritto all'autodeterminazione informativa degli atti amministrativi, ha

[267] Afferma testualmente la Suprema Corte: "Sebbene non sia ammissibile il diritto tipico alla riservatezza, viola il diritto assoluto di personalità, inteso quale diritto *erga omnes* alla libertà di autodeterminazione nelle svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito, ed ove non sussista, per la natura dell'attività svolta dalla persona e dal fatto divulgato, un preminente interesse pubblico di conoscenza".

[268] Cfr. Corte di Cassazione civile, sezione I, sentenza del 27 maggio 1975, n. 2129, in *Foro italiano*, 1976, fasc. I, c. 2895.

indotto il legislatore comunitario a prevedere in entrambe le normative l'adozione di sistemi e procedure atte a facilitare le operazioni di trattamento dati[269].

La CEDU, in particolare, all'art. 8, primo e secondo comma, contiene alcune disposizioni concernenti il riconoscimento del diritto di ogni persona fisica o giuridica al rispetto del bene della riservatezza, disponendo, nello specifico, che "ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui". Il "rispetto" richiesto dalla normativa CEDU, dunque, impone l'obbligo di non ingerenza nei diritti altrui e vincola gli Stati membri ad adottare misure idonee a garantire il rispetto della vita privata e familiare di ogni individuo, sia nei rapporti con lo Stato che nei rapporti con gli altri soggetti.

Il secondo comma dell'art. 8 in esame, in particolare, non autorizza a priori l'intervento dell'Autorità pubblica, tranne nei casi in cui sia la stessa legge in determinate circostanze – ossia quando sia necessario alla sicurezza nazionale e al benessere economico del Paese, oltreché per esigenze di protezione dei diritti e delle libertà individuali – a prevederne l'intervento.

Le norme convenzionali, quindi, in sostanza, finiscono con il concepire il diritto in esame alla stessa stregua della normativa nazionale, ossia come principio di libera autodeterminazione delle proprie scelte personali.

Le medesime finalità sono condivise anche dalla Convenzione n. 108 del 1981, la quale risulta finalizzata ad individuare adeguate misure di tutela dei diritti inviolabili della persona umana, atteso che l'obiettivo prioritario, sancito dall'art. 1, è quello di "garantire, sul territorio di ogni Parte, ad ogni persona fisica, qualunque siano la sua cittadinanza o residenza, il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, nei confronti

[269] Cfr. SCAGLIARINI S., *La riservatezza e i suoi limiti, sul bilanciamento di un diritto preso troppo sul serio*, cit., pp. 61 ss.

dell'elaborazione automatizzata dei dati di carattere personale che la riguardano ('protezione dei dati')". Ai fini del dettato convenzionale, in particolare, per "dati di carattere personale" deve intendersi, ai sensi dell'art. 2, "ogni informazione relativa ad una persona fisica identificata o identificabile".

L'art. 6, poi, specifica che "i dati di carattere personale indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altri credo, nonché i dati a carattere personale relativi allo stato di salute ed alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno non preveda garanzia adatte. Lo stesso dicasi dei dati di carattere personale relativi alle condanne penali".

La volontà del legislatore comunitario di istituire a favore di ciascun cittadino europeo, un sistema di protezione dei dati di natura personale "contro la distruzione accidentale o non autorizzata, ovvero la perdita accidentale così come contro l'accesso ai dati, la modifica o la diffusione non autorizzate" emerge chiaramente dalla portata dell'art. 7, con la precisazione, rinvenibile nell'art. 4, che "ogni Parte adotta, nel suo diritto interno, le misure necessarie per dare effetto ai principi fondamentali per la protezione dei dati […]".

Sempre in tema di tutela della riservatezza e della necessità di un suo contemperamento anche in ambito comunitario, occorre considerare anche la Direttiva del Parlamento Europeo e del Consiglio del 24 ottobre 1995 n. 46, emanata con l'obiettivo di conciliare la tutela della vita privata relativamente al trattamento dei dati personali con la libertà di circolazione dei medesimi. Conformemente alle disposizioni contenute in essa, l'art. 1 Capo I, stabilisce che "gli Stati membri garantiscono […] la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali". Di conseguenza, si impone agli Stati l'obbligo di adottare o modificare le loro legislazioni in materia di dati personali e in conformità alla legislazione comunitaria[270].

La Direttiva n. 46/95 CE è stata poi recentemente sostituita dal Regolamento n. 679 del 2016, che si è rivelato essere più esplicito della normativa precedente in quanto disciplina in maniera più armonica e definitiva la sfera dei dati riservati delle

[270] Si veda PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in Pardolesi R., *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, pp. 31 ss.

persone fisiche. La principale finalità che il regolamento si propone è quella di assicurare in tutta Europa, un livello coerente di tutela delle informazioni private e di prevenire eventuali disparità che ne possano ostacolare la libera circolazione nel mercato interno.

3.4. (*Segue*) L'evoluzione normativa degli ordinamenti europei in tema di tutela della *privacy*.

La tutela della riservatezza nella società dell'informazione ha assunto, nel corso degli anni, a seguito della stratificazione legislativa che via via si è andata creando, rilievo in una duplice direzione.

Innanzitutto, essa rileva quale strumento che garantisce all'individuo la libera costruzione della propria "sfera privata", come condizione per un pieno ed autonomo sviluppo della propria personalità, anche nell'ottica di un consapevole e libero esercizio dei diritti di partecipazione che caratterizzano la "sfera pubblica" del cittadino[271]. In secondo luogo, esso rileva quale strumento per l'esercizio di un controllo sociale diffuso e continuo sugli organismi pubblici e privati che raccolgono ed elaborano le informazioni, per assicurare la trasparenza della loro attività ed impedire la creazione di poteri incontrollati[272].

Questa evoluzione del concetto di *privacy* – rappresentata dalla dottrina già dalla seconda metà degli anni Sessanta – è stata definitivamente segnata da una serie di leggi di disciplina dell'attività di raccolta, elaborazione, diffusione dei dati personali, improntate al riconoscimento giuridico del diritto all'autodeterminazione informativa, emanate negli ordinamenti nazionali europei, in un processo di

[271] Peraltro, il concetto del diritto alla riservatezza può anche essere ulteriormente ampliato fino a ricomprendervi anche il diritto di escludere dalla propria sfera privata una determinata categoria di informazioni, il c.d. "diritto di non subire l'altrui impazienza comunicativa". Sul punto cfr. CERRI A., *Diritto alla riservatezza (diritto costituzionale)*, in *Enciclopedia giuridica*, XXVII, Roma, 1995, p. 3. Così inteso, dunque, il concetto di *privacy* viene ad essere inteso come diritto di controllare il flusso di informazioni riguardanti una persona sia "in uscita" sia "in entrata". In tal senso, cfr. RODOTÀ S., *Tecnologie e diritti*, cit., p. 122. Sul punto, cfr., altresì, BALDASSARRE A., *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974, pp. 471 ss., secondo il quale il concetto di *privacy* si estende al "dominio del contesto nel quale la persona agisce nell'esercizio delle proprie libertà fondamentali".

[272] Cfr. FARO S., *Trattamento dei dati personali e tutela della persona*, in *Digesto delle Discipline Pubblicistiche*, Torino, 2000, pp. 543-573.

reciproca influenza con iniziative assunte a livello internazionale e comunitario, a partire dal 1970.

La prima legge rilevante è quella del *Land* tedesco dello *Hesse* (Assia) del 1970, che regolamentava l'uso dei dati personali nello svolgimento automatizzato dei compiti della pubblica amministrazione[273]. Invece, la prima legge nazionale sulla protezione della riservatezza e sul controllo delle banche dati è quella svedese del 1973[274]. Sempre nel corso degli anni Settanta, sono stati molti gli Stati Europei che hanno proceduto con l'emanazione di norme in materia di tutela dei dati personali, a partire dalla Germania, a livello federale[275], seguita, poi, dalla Danimarca[276], dalla Norvegia[277], Francia[278], Austria[279] e Lussemburgo[280]. Negli anni Ottanta è la volta del Regno Unito[281], della Finlandia[282], dell'Irlanda[283], dei Paesi Bassi[284] e dell'Islanda[285]. Negli anni Novanta vengono varate la legge portoghese[286], quella spagnola[287] e quella belga[288].

Il percorso di elaborazione della normativa italiana sulla tutela dei dati personali, invece, è stato particolarmente lungo e tortuoso, ed ha occupato, con alterne vicende, quasi un ventennio di vita parlamentare[289]. Il nostro ordinamento,

---

[273] La legge è stata successivamente sostituita con una nuova versione dell'11 novembre 1996. Tuttavia, oggi, tutti i *Länder* hanno una propria normativa sulla protezione dei dati.Sul punto, in particolare, cfr. LOSANO M.G., *Introduzione*, in Giannantonio, Losano, Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla l. 675/1996*, Padova, 1997, p. XXIII.
[274] Si tratta della legge dell'11 maggio 1973, n. 289.
[275] Bundesdatenschutzgesetz del 27-1-1977, sostituita, poi, nel 1990, da una nuova legge: *Gesetz zur Fortentwicklung der Datenverarbeitung und des Daten Schutzes*, in vigore dal primo giugno 1991.
[276] Si tratta, in particolare, di due leggi emanate l'8 giugno 1978 relative una, la n. 293, al settore privato, l'altra, la n. 294, al settore pubblico.
[277] Cfr. la legge del 9 giugno 1978, n. 48.
[278] Cfr. La legge n. 78-17 del 6 gennaio 1978, rubricata *Loi relative à l'informatique aux fichiers et aux libertés*.
[279] Cfr. legge del 18 ottobre 1978, n. 565.
[280] Cfr. leggi del 30 marzo 1979 e 31 marzo 1979.
[281] Si tratta del c.d. *Data Protection Act*, del 12 luglio 1984.
[282] Cfr. legge n. 471 del 30 aprile 1987.
[283] Cfr. Legge del 13 giugno 1988, n. 25.
[284] Legge del 28 dicembre 1988, n. 665.
[285] Cfr. Legge del 28 dicembre 1989, n. 121.
[286] Legge del 29 aprile 1991, n. 10.
[287] C.d. *Ley organica 5/1992, de 29 de octubre, de regulacion del tratamiento automatizado de los datos de caracter personal*.
[288] Cfr. legge dell'8 dicembre 1992.
[289] La prima proposta di legge tendente a dare una disciplina organica alle banche dati risale infatti al 1981 e si deve all'on. Franco Accame (Atto Camera n. 2553 del 21 aprile 1981). Sul punto cfr. BUTTARELLI G., *Banche dati e tutela della riservatezza*: l*a privacy nella società dell'informazione: commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di*

invero, è giunto, nonostante i continui reclami da parte della dottrina[290], con notevole ritardo all'introduzione di una normativa minima in tema di tutela della persona nel trattamento dei dati. Tuttavia, il ritardo accumulato rispetto agli altri Paesi europei[291] ha però consentito, con l'approvazione della legge 675 del 1996[292], di fare entrare in vigore una disciplina particolarmente avanzata, tale da garantire un livello di tutela per molti aspetti superiore a quanto richiesto dai vincoli comunitari[293].

Orbene, tutte le normative e le regolamentazioni introdotte a partire dagli anni Settanta hanno subito, ovviamente, nel corso degli anni, continui aggiornamenti, frutto, sovente, delle esperienze maturate nell'applicazione della legislazione, dagli sviluppi della tecnologia informatica e telematica, dall'incremento dei flussi, anche transfrontalieri, dei dati, e dai vincoli derivanti dalle iniziative elaborate in seno al Consiglio d'Europa e dell'Unione Europea.

La letteratura giuridica in materia ha, nell'ottica di un'analisi comparatistica europea, tracciato una distinzione tra tre diverse generazioni di norme in tema di tutela dei dati personali[294]. È un percorso, quello seguito dai legislatori nazionali, infatti, nel quale è possibile individuare l'evoluzione da un approccio molto

trattamento dei dati personali e alla normativa comunitaria ed internazionale, Milano, 1997, pp. 101 ss.

[290] Sono tanti, infatti, i contributi della letteratura giuridica particolarmente critici nei confronti del *deficit* normativo in materia presente nel nostro ordinamento, dimostrativi, peraltro, di quanto fermento ci fosse nell'attesa dell'emanazione della legge n. 675 del 1996. Cfr., tra gli altri, Cfr. MIRABELLI G., *Le posizioni soggettive nell'elaborazione elettronica dei dati*, in *Diritto dell'informatica*, 1993, p. 313; MIRABELLI G., *In tema di tutela dei dati personali note a margine della proposta modificata di direttiva CEE*, in *Diritto dell'informatica*, 1993, p. 609; FROSINI V., *Note critiche al disegno di legge sulla protezione dei dati personali*, in *Diritto dell'informatica*, 1992, p. 745; LIBRANDO V., *La tutela della riservatezza nello sviluppo tecnologico*, in *Diritto dell'informatica*, 1987, p. 486; LOSANO G., *Un progetto di legge sulla protezione dei dati personali*, in *Diritto dell'informatica*, 1987, p. 465; GIANNANTONIO E., *Il progetto di legge sulle banche di dati personali e le normative straniere*, in *Giurisprudenza italiana*, 1985, fasc. IV, p. 168.

[291] Solo la Grecia è giunta all'approvazione della propria legge sulla tutela dei dati dopo il nostro Paese (legge n. 2472 del 19 marzo 1997), mentre gli altri Stati membri dell'Unione europea se ne erano dotati da tempo.

[292] Legge del 31 dicembre 1996, n. 675, rubricata "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", pubblicata in Gazzetta Ufficiale n. 5 dell'8 gennaio 1997, Supplemento Ordinario n. 3, entrata in vigore l'8 maggio 1997.

[293] LOSANO M.G., *I progetti di legge italiani sulla riservatezza dei dati personali*, in Alpa, Bessone (a cura di), *Banche dati, telematica e diritti della persona*, Padova, 1984, pp. 149 ss.

[294] Cfr., in particolare, PAGANO R., *Tutela dei dati personali: evoluzione della legislazione europea e stato del dibattito in Italia*, in *Informatica e diritto*, Milano, 1986, pp. 19 ss.

restrittivo – tipico delle leggi di c.d. "prima generazione"[295], come quella svedese nella prima versione del 1973 –, fondato su un regime di licenze ed autorizzazioni governative, risultando proibita ogni attività relativa alla elaborazione dei dati che non fosse espressamente permessa, ad un diverso modello, "di seconda generazione" – come quella francese, danese, norvegese ed austriaca –, incentrato sul regime della notifica o registrazione, in un apposito repertorio o registro, degli archivi e dei trattamenti dei dati, fondato sul principio della libertà dell'attività di raccolta e di elaborazione delle informazioni, limitata, o assoggettata a determinate condizioni, solo per certi aspetti, soprattutto con riguardo ai c.d. "dati sensibili". In particolare, le leggi appartenenti a questa seconda generazione si sono caratterizzate per aver esteso la tutela anche alle persone giuridiche e per aver recepito una serie di principi fondamentali in materia. La normativa italiana ha, infatti, desunto molti principi da questa normativa di seconda generazione e non ha solo preso spunto dalle esperienze applicative dei diversi ordinamenti europei, bensì ha anche recepito tutte le innovazioni determinate dalla repentina diffusione dei *personal computers*. In particolare, tra i diversi principi, sono stati recepiti nel nostro ordinamento, il principio della qualità dei dati – pertinenza, aggiornamento e completezza –, il principio di specificazione delle finalità della raccolta e della limitazione del suo uso allo scopo dichiarato, il principio di garanzia della sicurezza e del diritto di accesso ai dati cui si connette il passaggio da un modello basato sull'autorizzazione alla raccolta ad un modello fondato sulla registrazione, tramite notifica, in apposito registro[296].

Il legislatore italiano ha, così, considerato tutte le riflessioni elaborate non solo dalla dottrina italiana, ma anche dagli organismi sovranazionali, in particolare quelle afferenti gli effetti delle legislazioni in tema di *privacy* sugli organi di informazione e sulle imprese, e ha cercato di trovare il miglior bilanciamento possibile tra interessi, sovente confliggenti e spesso di medesimo rango costituzionale.

---

[295] Sul punto, cfr. PAGANO R., *Tutela dei dati personali: evoluzione della legislazione europea e stato del dibattito*, cit., p. 74.

[296] Cfr., in particolare, TRAVERSO A., *Il diritto dell'informatica*, cit., pp. 65 ss., il quale richiama la legge del 1° aprile 1985, n. 121, recante norme sul "Nuovo ordinamento dell'Amministrazione della Pubblica Sicurezza", la quale rappresenta il primo tentativo in Italia di regolamentazione in materia informatica.

Paradossalmente, proprio il fatto che il nostro ordinamento non avesse ancora una disciplina specifica del settore ha agevolato i lavori, in quanto non si è dovuto procedere ad una riforma della normativa, come avvenuto in altri Paesi, ma si è potuto semplicemente ricorrere ad un aggiornamento dei progetti e delle proposte di legge, già presentate, mediante un processo pressoché continuo. Basti pensare, infatti, che il disegno di legge – A. C. 1580 – presentato il 20 giugno del 1996 dal Governo altro non era se non il recepimento di tutti i risultati raggiunti nei lavori svolti durante le precedenti legislature. Di fatto, il disegno governativo presentato riproponeva espressamente il contenuto del disegno di legge del 1901, approvato dalla Commissione Giustizia della Camera dei Deputati nella passata legislatura, che a sua volta riassumeva gli aspetti principali del progetto governativo A.C. 1526 e delle proposte di iniziativa parlamentare dell'XI legislatura sulla tutela delle persone rispetto al trattamento dei dati personali.

La conferma del lungo *iter* formativo, senza soluzione di continuità, della legge in esame, in particolare, la si può trarre dal semplice raffronto delle Relazioni introduttive al disegno di legge 1526 (A.C.) ed al disegno di legge 1580 (A.C.) che, ad esempio, con riferimento al tema della "libertà informatica" ripropongono testualmente le stesse osservazioni.

Invero, la legge non contiene una definizione di libertà informatica, ponendosi, in ciò, in linea di continuità con le disposizioni internazionali, ma operando al contempo una sintesi tra le diverse opzioni che erano state proposte nei precedenti progetti di legge. Al contrario, essa si occupa di individuare i diritti degli interessati, in maniera tale da fornire loro una tutela effettiva in tema di trattamento dei dati personali, e riconosce, altresì, il diritto ad informarsi ed essere informati, cioè le prerogative dei gestori di banche dati, senza prospettare né una libertà assoluta di raccolta né irrigidendola in modo eccessivamente burocratico[297].

La *ratio* di tale scelta risiede nel fatto che l'obiettivo principale è stato quello di sancire la libertà di trattamento, ma sottoponendola a controlli adeguati onde salvaguardare la riservatezza di quei soggetti che si trovino nella condizione di dover fornire necessariamente i propri dati personali. Per fare un esempio pratico si

[297] Si trattava, d'altro canto, di temi che la dottrina già da tempo rivendicava. Cfr., in particolare, Cfr. LIBRANDO V., *La tutela della riservatezza nello sviluppo tecnologico*, cit., p. 488.

possono considerare quelle informazioni riservate che comunque devono essere fornite per poter beneficiare dei servizi assistenziali e previdenziali o commerciali. L'intento è stato, dunque, quello di non nascondere le informazioni, ma gestirle in maniera tale da non arrecare un pregiudizio ai diretti interessati e in maniera proporzionale rispetto alle ragioni del loro utilizzo.

Di talché, con la legge n. 675 del 1996 sul trattamento dei dati personali si è riconosciuto il diritto dell'interessato a controllare il flusso dei dati che lo riguardano, imponendo regole di comportamento a tutti coloro che effettuano operazioni su di essi. Per l'ordinamento italiano, l'approvazione della legge n. 675 nel 1996 ha segnato una tappa fondamentale in ordine alla definizione del diritto alla riservatezza, in quanto con essa si sono potuti superare i dibattiti dottrinari e si sono potuti recepire gli orientamenti giurisprudenziali che nel frattempo si erano andati sviluppando. Invero, questa legge ha portato, non solo, al definitivo superamento della concezione di riservatezza come "*right to be let alone*", per affermarsi come diritto all'autodeterminazione informativa, riconosciuto, ora, indistintamente in capo a tutti i cittadini, ma ha anche determinato un ampliamento della sfera di protezione: non più solamente le informazioni personali più delicate, quali quelle inerenti allo stato di salute e la vita sessuale, bensì tutti i dati comunque riferibili ad un soggetto[298].

La legge in esame, rientrante nella categoria della "terza generazione" di leggi sulla protezione dei dati, si connota soprattutto per le modalità mediante le quali viene realizzata la tutela. Atteso che il fine, infatti, è quello di consentire ai vari soggetti il controllo sull'utilizzo delle proprie informazioni personali, la maggior parte delle disposizioni di questa legge, lungi dal porre divieti, prevede una serie di adempimenti per l'utilizzo di tali dati, differenziati in ragione del soggetto utilizzatore, del tipo di dati trattati o delle operazioni che dovranno essere su di essi eseguite.

Dal punto di vista applicativo, la legge n. 675 riconosce tutela a tutti i trattamenti realizzati sui dati personali nel territorio dello Stato[299]. Orbene, per

[298] BUSIA G., *voce Riservatezza*, in *Digesto delle discipline pubblicistiche*, vol. XIV, Torino, 2000, pp. 436 ss.
[299] La legge precisa, altresì, all'art. 6 che anche il trattamento nel territorio dello Stato di dati personali detenuti all'estero è soggetto alle proprie disposizioni.

"dato personale", in particolare, a norma dell'art. 1, secondo comma, lettera c), deve intendersi qualsiasi informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Per "trattamenti", invece, ai sensi del secondo comma del medesimo art. 1, lettera b), deve intendersi qualunque operazione o complesso di operazioni svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati[300].

La legge n. 675 del 1996 fu emanata insieme alla legge del 31 dicembre 1996, n. 676, rubricata "Delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"[301], la quale delegava il Governo ad emanare, entro diciotto mesi dall'entrata in vigore della legge medesima, disposizioni integrative della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

Successivamente si è avvertita, poi, l'esigenza dell'elaborazione di un Testo Unico in materia, a causa dalle numerose modifiche succedutesi nell'arco di circa sette anni. Il Codice in materia di protezione dei dati personali, ossia il decreto legge del 30 giugno 2003, n. 196, il quale nasce proprio con lo scopo di riordinare la materia. Esso, tuttavia, non può definirsi un Testo Unico puro, posto che introduce anche alcune modificazioni e inserisce e sistematizza la giurisprudenza del Garante.

Il Codice ha ad oggetto, come la legge che lo ha preceduto, la protezione dei dati personali. È invalso l'uso di chiamarlo comunemente "Codice *privacy*" o "legge sulla *privacy*", posto che esso si connota per essere una legge sull'utilizzo delle informazioni e detta delle norme di natura essenzialmente procedurale sul

[300] Dalla disciplina generale della legge 675 restano esclusi solamente i dati anonimi, ossia quelli che, in origine o a seguito di trattamento, non possono essere associati ad un soggetto identificato o identificabile e che, proprio per tale ragione, non possono essere considerati come "personali", ai sensi del secondo comma, dell'art. 1, lettera i).

[301] Anche questa legge è stata pubblicata nel Supplemento Ordinario alla Gazzetta Ufficiale, dell'8 gennaio 1997, n. 5.

modo di utilizzare le informazioni, siano esse riservate o meno, sottolineando, dunque, la sua spiccata vocazione ordinamentale[302].

Si tratta di una legge che raramente vieta, ma che normalmente proceduralizza: esso, invero, ha la pretesa di disciplinare in modo organico sia gli aspetti sostanziali della materia, sia i profili istituzionali, sia le modalità evolutive di implementazione della disciplina di protezione dei dati personali nei diversi settori rilevanti[303], sia i profili concernenti il livello rimediale e sanzionatorio.

Ciò può facilmente evincersi dai principi generali della legge, che sono appunto l'art. 1, che sancisce il diritto alla protezione dei dati personali, l'art. 2, nel quale si afferma che il Testo Unico garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti delle libertà fondamentali, con particolare riferimento, ma non esclusivamente, al diritto alla riservatezza, all'identità personale e alla protezione dei dati personali. Questa disposizione evidenzia che i diritti della personalità che il Codice investe direttamente sono almeno tre: il diritto alla protezione dei dati personali; il diritto alla riservatezza; il diritto all'identità personale, i quali vanno bilanciati, a loro volta, con l'esigenza di semplificazione nell'adempimento degli obblighi da parte dei titolari e nell'esercizio dei loro diritti da parte degli interessati.

---

[302] Cfr. sul punto CALIFANO L., *Privacy: affermazione e pratica di un diritto fondamentale*, cit. p. 46. Rileva l'Autrice: "spesso richiamato anche come «Testo unico sulla *privacy*», questo organico *corpus* normativo prevede una serie di adempimenti anche molto dettagliati nei più svariati settori (ad esempio: sanitario, giudiziario, bancario, assicurativo, comunicazioni elettroniche)". La dottrina sul punto (cfr. CARTABIA M., *Le norme sulla privacy come osservatorio sulle tendenze attuali delle fonti del diritto*, in Losano (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001, pp. 59 ss.) ha anche rilevato che sia nella legge n. 675 del 1996, sia nel Codice per la protezione dei dati personali, "si condensano un po' tutte le tendenze dell'epoca contemporanea in tema di fonti del diritto: dall'impulso iniziale di matrice europea, alla collocazione del centro di produzione normativa nel Governo anziché nel Parlamento, alla istituzione di un presidio di settore, identificato in una autorità indipendente dotata anche di poteri normativi o paranormativi, alla previsione di un periodo di sperimentazione e di correlativi meccanismi di assestamento della riforma, all'affiancarsi di forme di produzione normativa autonoma accanto alle tradizionali fonti eteronome, allo sfumare di ogni netto confine distintivo tra il disporre e il provvedere, e così via. Dal punto di vista della tecnica della produzione normativa, la legislazione italiana sulla *privacy* costituisce un osservatorio privilegiato per le nuove problematiche in tema di fonti, che si riscontrano non solo nell'ordinamento italiano, ma un po' in tutti gli ordinamenti contemporanei, nei più svariati settori materiali".

[303] Cfr. GROSSO E., *Autorità indipendente o autorità onnipotente? Il potere normativo di fatto del Garante per la protezione dei dati personali*, in Losano (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001, pp. 139 ss.; SIMONCINI A., *Autorità indipendenti e costruzione dell'ordinamento giuridico: il caso del Garante per la protezione dei dati personali*, in *Diritto Pubblico*, fasc. 3, 1999, pp. 851 ss.

4. La tutela della *privacy* nell'era digitale.

Come più volte ribadito nel corso della stesura del presente elaborato, in questi anni si sta assistendo alla piena fioritura dell'*Internet of Things* e alla crescita dell'area della robotica dei servizi, che sfruttano dispositivi intelligenti in grado di dialogare tra loro o interfacciarsi con gli uomini, di raccogliere dati, analizzarli ed elaborarli in modo autonomo e interattivo, sempre più basati su algoritmi di *deep learning* programmati per decidere autonomamente la condotta da adottare.

Al contempo, ciò si è accompagnato anche alla rapida diffusione di quelli che abbiamo definito "*big data*" – ossia i sistemi basati su enormi quantità di dati digitali, raccolti attraverso la rete e i molteplici dispositivi tecnologici di uso comune, spesso analizzati ed elaborati in modo oscuro per gli interessati, vale a dire mediante l'impiego di algoritmi segreti –, di frequente utilizzati per assumere decisioni, compiere profilazioni o analisi predittive e che segnano il radicale cambiamento dei servizi legati all'informazione.

Tali fenomeni hanno finito con l'incidere enormemente sulla quotidianità degli individui, sempre più connotata dall'essere un continuo flusso di dati – per lo più personali – che può sfociare, talvolta, anche in forme di illecita manipolazione algoritmica degli stessi. Ben potrebbe accadere, ad esempio, che i dati di partenza utilizzati nei trattamenti algoritmici possano essere errati, imprecisi o incompleti; oppure, può anche accadere che gli algoritmi creati dai decisori umani, già in fase di progettazione, potrebbero illecitamente intervenire influenzare l'analisi e distorcere l'elaborazione, conducendo a risultati lesivi dei diritti e delle libertà individuali.

Va da sé che simili trattamenti, non solamente determinano la perdita di controllo da parte dell'interessato sui propri dati personali[304], ma possono, altresì, andare ad impattare su altri aspetti, come la riservatezza, la dignità umana, la libertà, l'autonomia e lo sviluppo delle persone, la sicurezza e la loro salute e implicare evidenti rischi di stigmatizzazione e discriminazione degli individui[305].

---

[304] Cfr. GIOVANNELLA F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, *I dati personali nel diritto europeo*, Milano, 2019, p. 1213.

[305] Sul punto, RODOTÀ S., *Il mondo della rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, pp. 37 ss.. L'Autore, in particolare, riflette sulla necessità di sottrarre la persona dalla "dittatura

Si è, dunque, posta l'urgenza di apprestare adeguati meccanismi di tutela della *privacy* e, più in generale, dei diritti e delle libertà degli individui contro illeciti trattamenti dei dati. Si è trattato, infatti, di definire le misure necessarie a minimizzare i rischi, prevenire i pericoli ed evitare i danni associati all'uso dei relativi trattamenti.

Facendo, dunque, riferimento alle soluzioni normative e alle esperienze applicative maturate negli ambiti dell'innovazione tecnologica, verificandone la trasponibilità ai nuovi scenari, pur sempre assumendo come prioritari i valori costituzionali e la protezione della persona umana, al fine di garantire la sicurezza della "società dell'algoritmo", si è ritenuto di adottare un approccio, ispirato ai principi di prevenzione e di precauzione, mediante la previsione di un articolato sistema di controlli a carico dei soggetti responsabili della progettazione, programmazione e utilizzo dei dati in ambito digitale, volti a ridurre i rischi ed evitare gli eventi dannosi per i diritti e le libertà degli individui, prima che ad eventualmente risarcirli.

Proprio in virtù di ciò, il legislatore europeo è intervenuto con il Regolamento 2016/679/UE, rubricato "Regolamento generale sulla protezione dei dati", per occuparsi, appunto del trattamento automatizzato dei dati personali, fronteggiando le lesioni che possono derivare dal trattamento di dati personali in violazione delle disposizioni regolamentari, in via prioritaria in termini di prevenzione, provvedendo all'allocazione dei relativi rischi e, solo in via subordinata, in termini di riparazione dei danni prodotti. Il modello di tutela introdotto, in particolare, si fonda sul principio di responsabilità dei soggetti attivi del trattamento di dati personali[306] connesso con l'attività commerciale o

dell'algoritmo", che presenta nuove insidie per i diritti e le libertà fondamentali degli individui, cui l'ordinamento sarà chiamato a dare nuove risposte.

[306] Sul punto, in particolare, FINOCCHIARO G., *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, pp. 289 ss.; FINOCCHIARO G., *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove Leggi Civili Commentate*, 2017, pp. 10 ss. Cfr., altresì, DI CIOMMO F., *Civiltà tecnologica, mercato e insicurezza: la responsabilità del diritto*, in *Rivista Critica di Diritto Privato*, 2010, p. 590. A parere dell'Autore, "siccome l'evoluzione scientifica e tecnologica, così come l'evoluzione dei mercati e la produttività delle imprese non possono essere generalmente impedite gravemente e ostacolate, l'unico principio che appare in grado di rispettare l'esigenza di promuovere tale evoluzione per incrementare il benessere della collettività e, allo stesso tempo, di ridurre al minimo i rischi derivanti dall'esposizione ai relativi pericoli, è quello di responsabilità". In senso conforme, D'AMBROSIO M., *Progresso tecnologico, "responsabilizzazione" dell'impresa ed educazione dell'utente*, Milano, 2017, p. 17, il quale parla

professionale[307] svolta, individuati, in via principale, nel titolare e, limitatamente, nel responsabile. In capo a tali soggetti vengono trasferiti i rischi derivanti dal trattamento automatizzato e i costi per arginare, in funzione preventiva, i danni ai diritti e alle libertà fondamentali della persona.

Come vedremo meglio nel prosieguo della trattazione, infatti, nella duplice direzione della massima responsabilizzazione degli autori del trattamento e di una maggiore valorizzazione dei profili di prevenzione dei possibili danni rileva una pluralità di puntuali obblighi di sicurezza[308] e controllo, posti dalla normativa europea principalmente a carico del titolare, a garanzia dei diritti degli interessati e della libera circolazione dei dati. Il Regolamento europeo estende significativamente la portata di tali obblighi, in cui si specifica la diligenza professionale alla quale sono chiamati gli autori del trattamento di dati, in primo luogo, in funzione della tutela dei diritti e delle libertà degli individui, ma anche della piena realizzazione delle finalità con esso perseguite.

di un dovere non positivizzato all'uso responsabile della rete, il fondamento del quale può essere rintracciato negli artt. 2, 21, 33 e 41 Cost.

[307] A norma dell'art. 2, paragrafo 2, lettera c), del Regolamento, si esclude espressamente dal suo ambito di applicazione i trattamenti effettuati per l'esercizio di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con l'attività commerciale o professionale svolta dal soggetto (considerando n. 18 Reg.).

[308] Cfr. BRAVO F., *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2018, pp. 775 ss.

CAPITOLO TERZO

La difficile convivenza tra *blockchain* e *data protection*.

SOMMARIO: 1. Il Regolamento "*General Data Protection Regulation*". - 1.1. (*Segue*) Il decreto legislativo n. 101 del 2018 di attuazione del GDPR. – 2. I soggetti della *blockchain* alla luce del Regolamento *Data Protection*. – 3. I Rapporti tra la tecnologia *blockchain* ed il Regolamento UE n. 679/2016 sulla protezione dei dati personali. – 3.1. (*Segue*) Il "dato personale" nel GDPR ed il c.d. "principio di minimizzazione dei dati". – 3.2. (*Segue*) I dati personali utilizzati nella tecnologia *blockchain*. – 3.3. (*Segue*) Anonimizzazione e pseudoanonimizzazione e chiavi pubbliche. – 4. Elementi di criticità tra la *blockchain* ed il GDPR. – 4.1. (*Segue*) L'operatività dei principi del GDPR nell'ambito della tecnologia *blockchain*. – 4.1.1. (*Segue*) Il principio di esattezza e di rettifica nel trattamento dei dati personali. – 4.1.2. (*Segue*) Il diritto di accesso. – 4.1.3. (*Segue*) Il diritto alla cancellazione ed il diritto all'oblio. – 5. Alcune potenzialità della *blockchain* a vantaggio della protezione dei dati personali. – 6. Il principio di *accountability* e la *blockchain*.

1. Il Regolamento "*General Data Protection Regulation*".

Il 25 maggio 2018 è divenuto applicativo anche in Italia il Regolamento (UE) 679/2016, ossia il Regolamento Generale sulla Protezione dei Dati, conosciuto anche come GDPR, dall'acronimo derivante dalla denominazione

inglese *General Data Protection Regulation*[309], che ha innovato radicalmente e per molti aspetti, la disciplina in materia di *privacy*, abrogando la Direttiva n. 95/46, che in Italia era stata recepita con l'emanazione del "Codice della *Privacy*" (ossia, il D.lgs. n. 196 del 2003).

La prima considerazione da fare, al fine di comprendere la reale portata della normativa in esame, è che la tecnologia costituisce ormai una parte consistente dell'esperienza contemporanea di una comunità civile; invero, il Considerando n. 6 si apre affermando che "La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali"[310]. A tal proposito, l'Unione Europea sottolinea come "[...] Le tecnologie dell'informazione e della comunicazione (TIC) non costituiscono più un settore a sé stante, bensì sono la base stessa di tutti i sistemi economici e delle società innovativi e moderni"[311].

La novità del GDPR consiste nell'aver considerato la compenetrazione cui oggi si assiste tra diritto ed informatica: in particolare, la norma giuridica richiede di incorporare il rispetto del diritto nelle piattaforme tecnologiche e nei processi organizzativi in modo che l'attività produttiva – la fornitura di beni e servizi o di prestazioni professionali – integri le cautele inerenti il trattamento dei dati personali[312]. Invero, come sancito dal Considerando n. 7 l'evoluzione cui si è assistito soprattutto negli ultimi anni "richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo

---

[309] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati), pubblicato in Gazzetta Ufficiale dell'Unione Europea L 119, del 4 maggio 2016, pp. 1-88.

[310] Prosegue il Considerando n. 6: "*La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali*".

[311] Cfr. Considerando 1, Proposta di Reg. UE relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'UE, COM(2017) 495, del 13 settembre 2017.

[312] Cfr. COSTANTINI F.*, Il regolamento (UE) 679/2016 sulla protezione dei dati personali*, in *Lavoro nella Giurisprudenza*, 2018, fasc. 6, p. 545.

dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche".

Il Regolamento, dunque, si fa portatore di una visione della protezione dei dati che ruota sul concetto di "*data management*", cioè sull'adozione preventiva di misure tecniche e organizzative adeguate al fine di raggiungere obiettivi di sicurezza e tutela nel trattamento dei dati personali. Tuttavia, non impone modelli prestabiliti ma individua una strada, menzionando principi e obiettivi cui tendere e raccomandando interventi che tengano conto "dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche"[313].

Esso, dunque, lascia ampia autonomia a coloro che sono chiamati ad applicare le disposizioni, imponendo, tuttavia, un limite rappresentato dalla responsabilità di contribuire alla creazione di un modello che sia effettivamente e tempestivamente in grado di rispondere alle esigenze di tutela. Per questo motivo, la portata del nuovo Regolamento sui dati ruota attorno a tre principi: *accountability*, a norma dell'art. 5 GDPR, *data protection by design* e *by default*, ai sensi dell'art. 25 GDPR[314].

In particolare, l'*accountability* è il c.d. principio di responsabilizzazione. Da una parte, esso si sostanzia nel riconoscimento di un'ampia autonomia in capo ai titolari del trattamento dei dati personali i quali, nel rispetto delle disposizioni di legge, possono conformare le misure da adottare in relazione alla propria realtà organizzativa; dall'altra parte si impone una disciplina della responsabilità dei titolari particolarmente rigida, mediante la previsione di sanzioni anche molto pesanti.

Accanto al principio di *accountability* si pone il principio di *privacy by design* il quale impone di adottare adeguate misure di protezione dei dati in tutte le

[313] A norma dell'art. 32 del GDPR.
[314] MONEA A., *Regolamento n. 2016/679: la necessità di uno specifico "modello organizzativo" per la protezione dei dati personali*, in *Azienditalia*, 2018, p. 1114; BECCARA J.L.A., *La privacy nel pubblico. Sintesi dell'integrazione tra codice italiano e regolamento europeo per la pubblica amministrazione*, Franco Angeli editore, Milano, 2018, p. 201.

fasi di progettazione del trattamento e di tutelare, comunque, mediante i mezzi più idonei, la *privacy* in tutto il procedimento posto in essere, in modo tale che la tutela dei dati divenga, in sostanza, una sorta di impostazione di *default*. Così facendo, dunque, il principio di *privacy by design* presuppone il principio di *privacy by default*, che nella sostanza si traduce nel dovere in capo ai gestori del servizio di stabilire a monte un utilizzo dei dati che si limiti, per impostazione predefinita – appunto, *by default* – ai soli casi necessari[315].

Mediante l'adozione di questi due principi, dunque, l'obiettivo è quello di creare un sistema di tutela preventiva, nella fase di progettazione, mediante una stabile organizzazione apposita, atto a prevenire i rischi e ad evitare la verificazione di danni nel processo di trattamento dei dati. Per definizione, infatti, il principio di *privacy by design* è volto a tutelare il dato sin "dal momento della progettazione" mentre il principio di *privacy by default* è volto a tutelare la vita privata per "impostazione predefinita"[316].

Ciò implica, allora, un generale ripensamento dell'organizzazione dei sistemi che si occupano del trattamento dei dati, i quali, d'ora innanzi, dovranno procedere ad articolare e distribuire adeguatamente le competenze in merito tra i vari uffici, al fine di recepire i dettami euro-unitari[317].

A tal fine, il Regolamento amplia i poteri delle Autorità garanti; viene, infatti, istituito un Comitato per le funzioni, con compiti di consulenza nei confronti della Commissione, a norma dell'art. 70 del GDPR, il quale risponde alla logica di esecuzione decentrata del diritto europeo, nell'ottica di incentivare ancora di più la cooperazione amministrativa[318]. Rilevanti sono, altresì, le previsioni che riguardano

---

[315] In particolare, cfr. sul punto CELELLA R., *Il principio di responsabilizzazione: la vera novità del GDPR*, in *Ciberspazio e diritto*, 2018, p. 211; ARCELLA G., *GDPR: il registro delle attività di trattamento e le misure di accountability*, in *Notariato*, 2018, p. 393.

[316] Cfr. FACCIOLI E., CASSARO M., *Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design*, in *Diritto Industriale*, 2018, fasc. 6, p. 561.

[317] FONDERICO G., *La regolazione amministrativa del trattamento dei dati personali*, in *Giornale di Diritto Amministrativo*, 2018, p. 415.

[318] A tal proposito risulta fondamentale menzionare la sentenza Schrems (Causa C-498/16, *Maximilian Schrems contro Facebook Ireland Limited*, del 25 gennaio 2018), nella quale il giudice sovranazionale ha sottolineato che le Autorità nazionali di controllo investite da una richiesta di protezione della *privacy* con riguardo al trattamento dei dati personali, devono poter verificare in piena indipendenza se il trasferimento di tali dati abbia rispettato i requisiti previsti dalla direttiva, anche in presenza di una decisione della Commissione sulla questione. Solo, infatti, quando il Comitato ricorre all'esercizio di poteri vincolanti, allora le Autorità non sono più sovrane nel garantire il rispetto delle regole europee sulla protezione dei dati.

l'istituzione di un responsabile dei dati personali, il quale è, in sostanza, un ufficio cui sono riconosciute funzioni di carattere consultivo e di controllo[319].

In generale, infatti, tutta la nuova organizzazione della tutela della *privacy* delineata dal Regolamento ruota attorno ad alcune figure chiave che stabilmente si occupano del compito della protezione dei dati: il titolare del trattamento/contitolare e il responsabile della protezione dei dati personali.

Il titolare, a norma dell'art. 4 del GDPR è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri (contitolari), determina le finalità e i mezzi del trattamento di dati personali, cioè tutte quelle operazioni applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

In sostanza, quindi, il titolare è colui che ha il compito di dare effettiva attuazione al GDPR, adottando comportamenti finalizzati specificamente alla tutela dei dati, progettando le linee strategiche più opportune e dimostrando così di rispettare il parametro di responsabilità nell'attuazione delle misure di protezione, così come richiesto dal Regolamento (principio di *accountability*). Costui sarà anche il responsabile dei risultati conseguiti, nonché di eventuali anomalie o vulnerabilità del sistema.

Dalla figura del titolare occorre distinguere quella del responsabile del trattamento, il quale si occupa, a norma del terzo paragrafo dell'art. 30 del GDPR, del registro dei trattamenti e, insieme al titolare, mette in atto le misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, così come imposto dall'art. 32 del GDPR. Inoltre, il titolare e il responsabile possono designare congiuntamente un responsabile della protezione dei dati personali, da cui l'acronimo RDP, o *Data Protection Officer* (DPO), di cui tratteremo nello specifico nel prosieguo della trattazione.

[319] Cfr. FIORENTINO L., *Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche*, in *Giornale di diritto amministrativo*, 2018, fasc. 6, p. 690.

1.1. (*Segue*) Il decreto legislativo n. 101 del 2018 di attuazione del GDPR.

Il 4 settembre 2018 sulla Gazzetta Ufficiale è stato pubblicato il D.lgs. del 10 agosto 2018, n. 101, con il quale, in attuazione della legge delega 25 ottobre 2017, n. 163, sono state adottate le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 che, in quanto tali sono obbligatorie e direttamente applicabili in ciascuno degli Stati membri.

Anche in quest'occasione, come si può evincere dalle date stesse, il legislatore italiano è intervenuto con un notevole e non trascurabile ritardo all'adeguamento, lasciando decorrere inutilmente il termine di due anni che il legislatore comunitario aveva assegnato per porre in essere il necessario adeguamento delle normative nazionali: infatti già l'art. 99 del Regolamento 2016/679, in vigore dal 24 maggio 2016, aveva indicato come data di applicazione quella del 25 maggio 2018.

Probabilmente sarebbe stato opportuno adottare la legge delega immediatamente dopo l'entrata in vigore del Regolamento, senza attendere gli ultimi mesi per emanare la delega e poi per dargli attuazione. Invece, dalla relazione illustrativa che accompagna il decreto risulta che la Commissione Ministeriale di studio per definire il contenuto della delega è stata istituita il 14 dicembre 2017 ed ha potuto iniziare i lavori il 4 gennaio 2018: quindi solo cinque mesi prima della data di applicazione del Regolamento[320].

La Commissione ministeriale inizialmente aveva predisposto una bozza recante nuove disposizioni, sostanzialmente finalizzate a precisare quelle fattispecie rispetto alle quali le norme del Regolamento presentavano margini di indeterminatezza e, al contempo, aveva proposto l'abrogazione integrale del Codice in materia di protezione dei dati personali di cui al D.lgs. n. 196/2003. Tuttavia, tale proposta non è stata accolta, dato che la soluzione adottata è stata quella di non abrogare per intero il Codice della *privacy*, ma di procedere sullo stesso mediante numerosi tagli e complesse riformulazioni, disattendendo, dunque, le indicazioni

[320] Cfr. CUFFARO V., *Quel che resta di un codice: il d.lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del Codice della Privacy al regolamento sulla protezione dei dati*, in *Corriere Giuridico*, 2018, fasc. 10, p. 1181.

provenienti dallo stesso Regolamento che, nel considerando n. 8, autorizzava espressamente gli Stati membri ad adottare provvedimenti legislativi "nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano"[321].

In particolare, la prima osservazione da fare riguarda il cambiamento del nome del Codice della *Privacy*, che ora risulta sicuramente pleonastico, in quanto eccessivamente lungo: "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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".

Dal punto di vista sostanziale, invece, vi è stato, anzitutto, un intervento di carattere manipolativo sul testo previgente del Codice della *Privacy* che ha interessato la Parte III. In particolare, le modifiche hanno riguardato la disciplina dei mezzi di tutela, secondo il principio della alternatività del reclamo al Garante o del ricorso all'autorità giudiziaria (art. 140 *bis*); la struttura organizzativa ed i compiti del Garante (artt. 153 -160) e l'impianto sanzionatorio (artt. 166 - 172).

L'intervento additivo, invece, ha riguardato il coordinamento delle disposizioni della Parte II del Codice, che riguardano il trattamento dei dati in specifici settori. In primo luogo, occorre sottolineare la modifica della stessa rubrica, divenuta oggi "Disposizioni specifiche per i trattamenti necessari per adempiere un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri nonché disposizioni per i trattamenti di cui al capo IX del regolamento". È stato introdotto il "Titolo 0.1", nel cui art. 45 *bis* si prevede che le norme successive devono essere accordate a quanto disposto dall'art. 6 del Regolamento in ordine alle condizioni di liceità del trattamento e all'art. 23 inerente le limitazioni dei diritti dell'interessato. E' stato abrogato il Capo I ed integrato il testo dell'art. 50 che costituiva l'unico contenuto del Capo II. Rimane in vigore l'art. 58 sul trattamento dei dati ai fini di sicurezza nazionale ed i

[321] Il decreto in esame in particolare è intervenuto abrogando 110 articoli, sostituendone 35, modificandone 29 ed aggiungendone altri 29 di nuovi.

successivi artt. da 59 a 61 nei quali sono dettate le disposizioni in tema di accesso ai documenti amministrativi.

L'intervento demolitorio ha riguardato, invece, in maniera radicale la Parte I: è rimasto in vigore il solo art. 1 del Titolo I, che ribadisce che il trattamento dei dati avviene secondo le norme del regolamento e del codice, e l'art. 2 che ribadisce che il Codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del regolamento.

Complessivamente, la tecnica utilizzata per l'armonizzazione del Codice ai dettami del Regolamento europeo non può dirsi del tutto riuscita, atteso che l'intervento a macchia di leopardo posto in essere non consente certamente un'agevole interpretazione ed applicazione delle norme del Codice ora riformato, rendendo auspicabile, quindi, l'emanazione in tempi celeri di un testo coordinato che tenga conto di tutte le modifiche intervenute[322].

2. I soggetti della *blockchain* alla luce del Regolamento *Data Protection*.

Il primo aspetto da considerare nel valutare le modalità di applicazione della disciplina in materia di protezione dei dati personali introdotta dal GDPR alle *Distribuited Ledger Technology*, come la *blockchain*, riguarda l'individuazione dei ruoli svolti dai partecipanti al *network*, alla luce delle definizioni fornite dal Regolamento europeo in relazione ai diversi soggetti agenti nel processo di trattamento dei dati personali.

Anzitutto, occorre considerare che il Regolamento GDPR opera una distinzione tra diverse tipologie di soggetti, a cui sono associati diritti ed obblighi particolari. In particolare, rileva, in primo luogo, la figura dell'"interessato", che è la persona fisica a cui i dati si riferiscono. In particolare, il Regolamento disciplina

[322] Cfr. NUCCI G., *GDPR: struttura e contenuti del d.lgs. n. 101/2018*, in *Azienditalia*, 2018, fasc. 10, p. 1237

i "diritti dell'interessato" nel Capo III, agli articoli che vanno dal 12 al 23[323]. La formula "diritti dell'interessato" indica l'insieme dei poteri, delle facoltà e dei rimedi che compongono il contenuto del diritto alla protezione dei dati personali[324], riconosciuto come diritto fondamentale dei cittadini dell'Unione europea dagli articoli 8 della Carta dei diritti fondamentali dell'Unione europea e 1 del Regolamento[325].

Orbene, con la locuzione "diritti dell'interessato" si designa, dunque, una serie di prerogative di natura diversa, ora facoltà e poteri sostantivi, ora rimedi di

[323] In particolare, sui "diritti dell'interessato" alla luce del GDPR cfr. PIRAINO F., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuova Giurisprudenza Commentata*, 2017, pp. 394 ss.; RICCI A., *I diritti dell'interessato*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, opera diretta da Finocchiaro, Bologna, 2017, pp. 179 ss.; CALISAI F., *I diritti dell'interessato*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 327 ss.; DI CIOMMO F., *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 353 ss.; SAMMARCO P., *Privacy digitale, motori di ricerca e social network: dal diritto di accesso e rettifica al diritto all'oblio condizionato*, in Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, pp. 157 ss.; BATTELLI E., D'IPPOLITO G., *Il diritto alla portabilità dei dati personali*, in Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, pp. 185 ss.; GIOVANNANGELI S.F., *L'informativa agli interessati e il consenso al trattamento*, in 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, pp. 99 ss.; MONTANARO D., *Il diritto di accesso ai dati personali e il diritto di rettifica*, in 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, pp. 185 ss.; BERTI SUMAN A., *Il diritto alla cancellazione*, in 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, pp. 199 ss.; CRISTOFARI E., *Il diritto alla limitazione del trattamento*, in 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, pp. 215 ss.; BIANCHI L., *Il diritto alla portabilità dei dati*, in 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, pp. 223 ss.; SENIGAGLIA R., *Il Reg. UE 2016/679 e il diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Leggi Civili Commentate*, 2017, pp. 1023 ss.; TORINO R., *Il diritto di opposizione al trattamento dei dati personali e il diritto a non essere sottoposti a decisioni basate su trattamenti automatizzati e alla profilazione nel Regolamento (UE) 2016/679*, in *Cittadinanza europea*, 2018, pp. 45 ss.; FRAIOLI M., *Il diritto di opposizione e la revoca del consenso*, in *Cittadinanza europea*, 2018, pp. 239 ss.; BOZZOLI J., *La portabilità dei dati personali*, in *Ciberspazio e diritto*, 2019, pp. 133 ss.; MONTELEONE A.G., *Il diritto alla portabilità dei dati. Tra diritti della personalità e diritti del mercato*, in *Luiss law review*, 2017, pp. 202 ss.

[324] Sul punto cfr. RODOTÀ S., *Controllo e privacy della vita quotidiana. Dalla tutela della vita privata alla protezione dei dati personali*, in *Rivista Critica di Diritto Privato*, 2019, pp. 9 ss.

[325] Sulla natura fondamentale del diritto alla protezione dei dati personale cfr. GAMBINI M., *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *Espaço Jurídico*, 2013, pp. 149 ss.

natura specifica[326], ai quali la disciplina europea affida il compito di consentire all'interessato di seguire, di controllare e di indirizzare la circolazione delle proprie informazioni di carattere personale[327].

Vi è, poi, il Titolare del trattamento, come prima accennato, ossia, a norma del primo comma, n. 7 dell'art. 4 del Regolamento *de quo*, "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali"; ancora, il "Responsabile del trattamento", il quale è individuato dal successivo n. 8 del primo comma dell'art. 4 in commento, come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

Oltre a queste figure che potremmo definire "principali" è altresì previsto che i dati possano essere comunicati anche a dei "destinatari", mentre sono definiti "terzi" tutti coloro che non rientrano in una delle definizioni precedenti, a norma del n. 10 del primo comma dell'art. 5 del Regolamento.

---

[326] Il merito di aver suggerito la chiave di lettura rimediale per alcune delle prerogative riconosciute all'interessato della disciplina sul trattamento dei dati personali va riconosciuto a diversi Autori. In particolare, cfr. DI MAJO A., *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in Cuffaro, Ricciuto, Zeno-Zencovich (a cura di), *Trattamento dei dati personali e tutela della persona*, Milano, 1998, pp. 236 ss., il quale suggerisce di adoperare la categoria dei "diritti-rimedi". Cfr., altresì, PIRAINO F., *La liceità e la correttezza*, in Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, 2006, pp. 787 ss.; VECCHI P., *Art. 1- Finalità e definizioni*, in Bianca, Busnelli (a cura di), *Tutela della privacy. Commentario alla legge 31 dicembre 1996, n. 675*, in *Leggi Civili Commentate*, 1999, pp. 236 ss. Afferma, invece, LO SURDO C., *Gli strumenti di tutela del soggetto "interessato" nella legge e nella sua concreta applicazione*, in Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, 2018, I, p. 620, che "una classificazione dogmatica [...] è possibile solo una volta che ne siano esaminate le concrete modalità operative".

[327] Sul punto cfr. CASTRONOVO C., *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Europa diritto privato*, 1998, pp. 653 ss.; DI MAJO A., *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, cit., pp. 225 ss.; VETTORI G., *Privacy e diritti dell'interessato*, in *Responsabilità Civile e Previdenza*, 1998, pp. 885 ss.; BARGELLI E., *Art. 13 - Diritti dell'interessato*, in Bianca, Busnelli (a cura di), *Tutela della privacy. Commentario alla legge 675/96*, in *Leggi Civili Commentate*, 2019, pp. 394 ss.; NERVI A., *I diritti dell'interessato*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *Il Codice del trattamento dei dati personali*, Torino, 2007, pp. 61 ss.; MORMILE L., *I diritti dell'interessato*, in Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, 2006, pp. 1199 ss.; LO SURDO C., *Gli strumenti di tutela del soggetto "interessato" nella legge e nella sua concreta applicazione*, in Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, I, Milano, 2003, pp. 617 ss.; SALZANO G., *I diritti dell'interessato*, in Monducci, Sartor (a cura di), *Il codice in materia di protezione dei dati personali. Commentario sistematico al D.Lgs. 30 giugno 2003 n. 196*, Padova, 2004, pp. 19 ss.

Orbene, calando, ora, l'operatività di queste figure nell'ambito della tecnologia *blockchain*, occorre osservare come l'individuazione dei ruoli svolti dai partecipanti è differente a seconda che si tratti di una *blockchain* chiusa o aperta.

Nel caso di *blockchain* chiusa, ossia in caso di *blockchain permissioned*, è possibile individuare due casi[328]. Il primo caso è quello di un singolo (persona fisica o ente) che decide di partecipare ad un consorzio che gestisce una *blockchain* chiusa. Ciò significa che tale soggetto dovrà premunirsi ed accettare la circostanza che tutti i partecipanti potranno trattare i dati che andrà ad immettere nel *network* e che potrà essere responsabile di validare transazioni degli altri, trattando quindi i dati personali da essi immessi nella *blockchain*. In tale ipotesi sembra configurabile la fattispecie di contitolarità del trattamento (secondo quanto previsto dall'art. 26 GDPR), ossia la situazione in cui il trattamento viene effettuato congiuntamente da due titolari. In tale ipotesi la norma prevede che i soggetti si accordino per definire reciproche responsabilità e rispettive funzioni al fine di garantire il rispetto delle prerogative degli interessati[329].

Il secondo caso riguarda, invece, l'ipotesi in cui un consorzio offra servizi agli utenti finali basati su una *blockchain permissioned*, registrando i dati personali su tale strumento. Anche in tali ipotesi sembra che la soluzione più semplice sia quella di individuare una contitolarità del trattamento in capo ai partecipanti al consorzio, mentre gli utenti finali saranno inquadrati come interessati.

La soluzione della contitolarità del trattamento appare la più ragionevole ed implica che vengano stabiliti in maniera preventiva i ruoli, le responsabilità e le modalità con cui saranno adempiuti gli obblighi previsti dal GDPR.

In dottrina, in realtà, vi è anche chi ritiene che in una *blockchain* privata i nodi (ossia i vari partecipanti) andrebbero qualificati alla stregua di Responsabili del trattamento, più che Titolari o contitolari, quali intermediari che elaborano ed utilizzano i dati registrati sulla *blockchain*. A parere di tale parte della dottrina,

---

[328] Cfr. IBÁÑEZ, KIERON O'HARA L.D., SIMPERL E., *On Blockchains and the General Data Protection Regulation*, in *https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf*, 2018, par. 5.

[329] Cfr. MANTELERO A., *GDPR tra novità e discontinuità - Gli autori del trattamento dati: titolare e responsabile*, in *Giurisprudenza Italiana*, 2019, fasc. 12, p. 2777.

tuttavia, vi sarebbe comunque la necessità che siano definiti i ruoli dei partecipanti all'interno di un apposito "*distributed ledger's government arrangements*"[330].

Più complicato, invece, risulta decifrare i ruoli delle parti per una *blockchain permissionless* (come *Bitcoin*). Come abbiamo precedentemente visto, infatti, questa tipologia di *blockchain* si connota per essere del tutto decentralizzata ed aperta; non sono presenti dei soggetti che "autorizzano" l'accesso al *network* e che "determinano finalità e mezzi del trattamento" dato che per poter inserire transazioni è sufficiente reperire gli appositi *software* e creare le chiavi crittografiche. "I ruoli che possono essere individuati all'interno di tali *blockchain* variano a seconda delle elaborazioni che vengono svolte: un *fullnode* conserva localmente l'intera *blockchain* (ed i dati personali in essa registrati) mentre un *lightweight node* si limita a scaricare gli *header* delle transazioni per verificare l'autenticità delle stesse. Un nodo *miner* dal canto suo elabora i blocchi, processando i dati in essi contenuti. A dispetto di tali diversi ruoli rimane fermo il fatto che in una *blockchain permissionless* non è possibile individuare un unico punto di controllo del *network*, operando lo stesso secondo un criterio *peer-to-peer*, decentralizzato e distribuito"[331].

Tenendo conto di quanto detto, dunque, alcuni Autori[332] sono arrivati a ritenere che ciascun nodo della *blockchain* pubblica andrebbe qualificato come titolare del trattamento, posto che ogni nodo non è soggetto ad istruzioni esterne, decide autonomamente di aderire al *network* e persegue i propri obiettivi, mentre sarebbe da escludersi un'ipotesi di contitolarità del trattamento in quanto non vengono congiuntamente definite le modalità e scopi dello stesso e, pur essendo la *blockchain* creata dal comportamento dei vari nodi, ciascuno non può determinare le modalità di trattamento degli altri.

Sebbene tale ricostruzione risulti senz'altro apprezzabile, tuttavia, espone il fianco ad alcune critiche di non facile superamento. In primo luogo, risulta alquanto

---

[330] Cfr. SARZANA DI S.IPPOLITO F., NICOTRA M., *Diritto alla blockchain, intelligenza artificiale e IOT*, Milano, 2018, pp. 74 ss.
[331] Cfr. SARZANA DI S.IPPOLITO F., NICOTRA M., *Diritto alla blockchain, intelligenza artificiale e IOT*, cit., p. 75.
[332] Cfr. FINCK M., *Blockchains and Data Protection in the European Union*, *Max Planck Institute for Innovation & Competition Research Paper* No. 18-01, in *European Data Protection Law Review*, 1/2018, pp. 26 ss.

complicato stabilire l'esatto numero e la reale collocazione dei vari nodi partecipanti ad una *blockchain* pubblica. In secondo luogo, i nodi, a ben vedere, si configurano come dei soggetti passivi, dato che le modalità di gestione del *network* sono dettate dal *software* creato dagli sviluppatori; essi accedono solamente ai dati cifrati o risultanti dall'applicazione della funzione di *hash* e non sono in grado di apportare alcuna modifica alla *blockchain*. L'esercizio dei diritti riconosciuti dal GDPR in tale ipotesi di titolarità diffusa, risulterebbe, inoltre, assai difficoltoso per gli interessati, che dovrebbero contattarli tutti singolarmente. Si pone, inoltre, l'oggettiva difficoltà di applicare gli obblighi di informativa di cui all'art. 13 GDPR, i principi di liceità del trattamento secondo un'opportuna base giuridica, a norma dell'art. 6 GDPR, gli obblighi previsti per la sicurezza dei trattamenti, ai sensi dell'art. 32 GDPR, nonché la disciplina del trasferimento dei dati personali in Stati extra-UE[333].

A tale ricostruzione ermeneutica, si è contrapposta una diversa soluzione[334], la quale procede distinguendo due diverse ipotesi. La prima riguarda il caso in cui un singolo interagisce direttamente con una *blockchain permissionless*, ad esempio effettuando transazioni di criptovalute. In tale fattispecie non sarà possibile configurare la sussistenza di un titolare unico del trattamento. Per tale ragione si è proposto di collocare la responsabilità della conformità al GDPR direttamente sugli utenti stessi nel senso di: a) proibire l'inserimento di determinate categorie di dati personali; e b) prevedere che i medesimi abbiano ottenuto il consenso o trattino i dati in forza di altra base giuridica.

La seconda ipotesi, invece, riguarda quelle applicazioni che usano una *blockchain permissionless* come *back-end*. È la situazione in cui un interessato interagisce con un'applicazione che utilizza una *blockchain* aperta come *back-end*. Coloro che gestiscono l'applicazione intermedia possono essere qualificati come titolari del trattamento – in quanto ne definiscono l'ambito ed i mezzi, decidendo quali dati vengono registrati sulla *blockchain* –. Saranno quindi obbligati a porre in essere gli adempimenti previsti dal GDPR nei confronti dei vari interessati.

---

[333] Cfr. SARZANA DI S.IPPOLITO F., NICOTRA M., *Diritto alla blockchain, intelligenza artificiale e IOT*, cit., p. 76.
[334] Cfr. IBÁÑEZ, KIERON O'HARA L.D., SIMPERL E., *On Blockchains and the General Data Protection Regulation*, cit., par. 5.

Orbene, se le soluzioni così individuate per l'individuazione dei ruoli all'interno di *blockchain permissioned* sembrano soddisfacenti, quelle relative alle *blockchain* aperte lasciano adito ad alcune considerazioni.

Innanzitutto, va da sé che un utente che effettua delle transazioni sulla *blockchain* è necessariamente titolare dei dati personali che egli stesso immette. D'altra parte, qualora una persona fisica si limiti, ad esempio, ad effettuare transazioni in criptovalute, senza neanche partecipare come nodo alla *blockchain* o comunque operando come *lightweight node*, il trattamento del dato personale pseudonimizzato consistente nella chiave pubblica del destinatario della transazione potrebbe essere escluso dall'ambito di applicazione materiale del GDPR, il cui art. 2 prevede la non applicabilità del Regolamento quando per i trattamenti di dati personali "effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico".

Qualora invece la persona fisica effettui il trattamento per scopi diversi da quelli indicati dall'art. 2 GDPR si configurerà come titolare del medesimo. In tal caso dovrà porre in essere gli adempimenti previsti dalla normativa, tra cui rendere l'informativa agli interessati, *ex* articoli 13 e 14 GDPR, trattare i dati in forza di una valida base giuridica – che nel caso di transazioni in criptovalute potrà anche risiedere nell'adempimento ad un contratto intercorso con il destinatario della transazione – limitandosi ad effettuare i trattamenti necessari al perseguimento delle finalità dichiarate, garantendo altresì la sicurezza dei sistemi da essa utilizzati, nel senso che dovrà garantire di non diffondere dati ulteriori sulla *blockchain* rispetto a quelli necessari e che gli strumenti personali utilizzati siano conformi ai criteri di sicurezza stabiliti dalla normativa e dalle buone pratiche[335]. In tal caso inoltre, gli interessati potranno esercitare i diritti previsti dal GDPR direttamente nei confronti di tale titolare.

Anche la disciplina di coloro che operano quali nodi, limitandosi quindi a processare le informazioni della *blockchain* secondo le modalità previste dal *software* utilizzato, potrebbe essere parzialmente diversa da quella esaminata in precedenza.

---

[335] Cfr. SARZANA DI S.IPPOLITO F., NICOTRA M., *Diritto alla blockchain, intelligenza artificiale e IOT*, cit., p. 76.

Innanzitutto, in presenza di dati personali pseudonimizzati, come vedremo nel prosieguo della trattazione, il Considerando n. 26, sulla scorta della giurisprudenza europea, precisa che è necessario considerare i mezzi – intesi come fattori obiettivi, in cui vi rientrano i costi, le risorse ed il tempo necessario – che il titolare o un terzo può utilizzare per identificare l'interessato. Ebbene, tale precisazione potrebbe portare ad escludere la qualificazione alla stregua di titolari del trattamento di quei soggetti che si limitino ad operare come nodi (*lightweight*, *full* o *miners*) senza avere i mezzi (economici e tecnologici) per poter procedere alle complesse operazioni necessarie a risalire all'identificazione di coloro che partecipano alla *blockchain* aperta (quali analisi di multiple transazioni, individuazione degli IP, ecc.). E' evidente, invece, che chi effettua tali attività[336] dovrà essere qualificato titolare del trattamento nel momento in cui risale ai dati identificativi degli interessati, e come tale sarà obbligato ad adempiere alle prescrizioni del GDPR.

In secondo luogo, anche in una prospettiva *de jure condendo*, considerando che i nodi che operano quali *miners* svolgono la loro attività a fronte di un guadagno (che deriva sia dal "premio" derivante dal meccanismo di consenso e sia dagli incentivi che coloro che vogliono effettuare la transazione spesso mettono loro a disposizione) i medesimi potrebbero essere identificati quali prestatori di servizi della società dell'informazione, con conseguente applicazione della disciplina di cui alla Direttiva n. 2000/31/CE[337] (e delle relative norme di recepimento nazionali) ed in particolare delle regole previste per il c.d. *mere conduit*, il *caching* e l'*hosting* delle informazioni, nonché di quanto previsto dalla Direttiva n. 58/2002/CE[338] che prevede una disciplina specifica per il trattamento dei dati personali nel settore delle comunicazioni elettroniche.

Ciò consentirebbe di identificare in maniera più certa coloro che sono i titolari del trattamento dei dati nell'ambito di una *blockchain permissionless*,

[336] Come, ad esempio, i *Blockchain Service Provider* che già offrono servizi di identificazione degli utenti.
[337] Direttiva dell'8 giugno 2000, n. 2000/31/CE, rubricata "Direttiva del Parlamento europeo e del Consiglio relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico")", pubblicata nella Gazzetta Ufficiale della Comunità Europea del 17 luglio 2000, n. L 178 ed entrata in vigore il 17 luglio 2000.
[338] Concernente la tutela dei dati personali nell'ambito del settore delle comunicazioni elettroniche.

considerato anche che l'applicabilità del GDPR al di fuori dell'Unione Europea è limitata ai titolari che offrono beni o prestano servizi a interessati che si trovano nell'Unione "indipendentemente dall'obbligatorietà di un pagamento dell'interessato" o che monitorano il comportamento degli stessi, con conseguente autorizzazione da parte dei soggetti così individuati a trattare i dati necessari a realizzare la comunicazione per tutta la durata necessaria a tal fine.

Accanto alle problematiche sin qui sollevate, la definizione dei ruoli dei soggetti che partecipano ad una *blockchain* nell'ottica del diritto alla protezione dei dati personali consente, altresì, di esaminare gli ulteriori aspetti e le questioni che tale disciplina comporta con riferimento all'operatività dei soggetti residenti al di fuori del territorio euro-unitario.

Come appena accennato è noto che il Regolamento Europeo non limita la propria applicazione ai soggetti che hanno uno stabilimento nell'Unione Europea, bensì estende la propria portata anche nei confronti di soggetti residenti extra-UE, i quali sono obbligati, qualora il trattamento riguardi persone fisiche che si trovano nel territorio dell'Unione e tale trattamento consista nell'offerta di beni o servizi, indipendentemente dal pagamento di somme di denaro o nel monitoraggio degli interessati, ad applicare la disciplina prevista nel GDPR.

Tale previsione, nell'ambito di una *blockchain permissionless*, può comportare alcuni problemi soprattutto con riferimento alla difficoltà di identificare effettivamente coloro che effettuano i trattamenti al di fuori dell'Unione Europea, stante la naturale propensione di tali *network* ad assumere proporzioni internazionali.

A maggior ragione, considerando che ciascun nodo può conservare localmente l'intera *blockchain*, si pongono problemi di applicabilità della disciplina relativa al trasferimento dei dati in Paesi extra-UE, consentito solo nel rispetto delle condizioni di cui al Capo V del Regolamento. Ciò, sostanzialmente, comporterebbe l'onere in capo a ciascun titolare del trattamento per cui ogni volta che inserisce dati in una *blockchain* pubblica, dovrebbe andare poi a verificare l'esistenza delle

condizioni stabilite dal GDPR (decisioni di adeguatezza, clausole di salvaguardia) verso destinatari a lui sconosciuti[339].

3. I Rapporti tra la tecnologia *blockchain* ed il Regolamento UE n. 679/2016 sulla protezione dei dati personali.

L'entrata in vigore del nuovo Regolamento UE n. 679/2016 relativo alla protezione dei dati personali ha portato diversi Autori a domandarsi se la tecnologia *blockchain* possa ritenersi compatibile con le nuove disposizioni regolamentari, in particolar modo per le caratteristiche di decentralizzazione, immodificabilità e persistenza dei dati registrati, i quali ben potrebbero venirsi a porre in contrasto con alcuni dei diritti riconosciuti agli interessati, ossia alle persone fisiche cui i dati si riferiscono, e con i principi posti dalla nuova disciplina[340], tanto da indurre l'*EU Blockchain Observatory and Forum* a dedicare un apposito *workshop* sulla tematica[341].

---

[339] Diverso il discorso in una *blockchain permissioned* in cui, tendenzialmente, tutti i partecipanti sono identificati o identificabili.

[340] Sui rapporti tra *blockchain* e GDPR cfr. BOLDRINI N., *Blockchain e GDPR: le sfide e le opportunità per la protezione dei dati*, in *https://www.blockchain4innovation.it/sicurezza/ blockchain -gdpr/*, 2018; NICOTRA M., *Blockchain e GDPR: le norme da conoscere per tutti i problemi*, in *https://www.agendadigitale.eu/sicurezza/blockchain-e-gdpr-le-norme-da-conoscere-per-tutti-i-problemi/*, 2018; GAROFALO L., *GDPR, e se la Blockchain non fosse conforme al regolamento?*, in *key4biz.it/gdpr-e-se-la-blockchain-non-fosse-conforme-al-regolamento /222368/*, 2018; MAXWELL W., SALMON J., *A guide to blockchain and data protection*, in *https://www. hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf*, 2018; FINCK M., *Blockchains and Data Protection in the European Union*, *Max Planck Institute for Innovation & Competition Research Paper*, cit., pp. 17 ss.; IBÁÑEZ, KIERON O'HARA L.D., SIMPERL E., *On Blockchains and the General Data Protection Regulation*, cit.; PIATTI L., *Blockchain, decentralizzazione e privacy: un nuovo approccio del diritto*, in *Ciberspazio e diritto*, vol. 19, n. 60, 2018, pp. 179-196; RAZZINI A., *Blockchain e protezione dei Dati personali alla luce del nuovo regolamento europeo GDPR*, in *Ciberspazio e diritto*, vol. 19, n. 60, 2018, pp. 197-208.

[341] Cfr. *https://www.eublockchainforum.eu/video/workshop/gdpr-june-8th-2018-workshop-part-3-working-session*.

Giova rammentare, in particolare, il *report* "*Blockchain Innovation Europe*" del 21 agosto 2018 redatto dall'*European Union Blockchain Observatory and Forum* che sottolinea come la tecnologia *blockchain* sia in realtà ancora immatura e che probabilmente, evolvendo, sarà più semplice conciliarla con quanto previsto dal Regolamento. Sono in elaborazione, infatti, nuove tecniche finalizzate ad una maggiore protezione dei dati personali che eliminano la possibilità di risalire al singolo. Questo dovrebbe persuadere il legislatore a far operare tutte le eccezioni previste dal GDPR in modo da evitare che un'interpretazione troppo restrittiva possa comportare un freno all'innovazione

Occorre, comunque, rilevare che la tecnologia *blockchain* è stata anche considerate una valida alternativa per la gestione dei dati personali certamente più conforme ai principi della *privacy* dei singoli[342], come vedremo più dettagliatamente nel prosieguo del lavoro, posto che essa consente di fornire, al momento dell'accesso ad un servizio *online*, solo le informazioni strettamente necessarie all'erogazione dello stesso oppure di modulare il consenso per determinati trattamenti specifici, consentendo al contempo anche di conservare traccia del c.d. "Consenso 2.0" in modo da consentirne la verifica da parte di diversi attori[343].

Orbene, come sottolineato da parte della dottrina[344], il conflitto che potrebbe aprirsi tra quanto disposto dalle nuove norme del GDPR e la tecnologia *blockchain* deriva principalmente dall'impostazione concettuale del Regolamento europeo, il quale è diretto a regolamentare le ipotesi di trattamento centralizzato dei dati personali – i c.d. "*data silos*" – che lo rende, quindi, difficilmente adattabile ad una tecnologia che si fonda sulla decentralizzazione e distribuzione su un *network* delle operazioni computazionali[345].

Di talché, il quesito che occorre porsi riguarda la tematica sul se nella *blockchain* vengano "normalmente" trattati dati personali, tenendo conto della definizione data dal GDPR.

3.1. (*Segue*) Il "dato personale" nel GDPR ed il c.d. "principio di minimizzazione dei dati".

Per poter rispondere al quesito poc'anzi posto, occorre, in primo luogo chiedersi cosa il GDPR intenda per "dato personale".

---

[342] Si veda ZYSKIND G., NATHAN O., PENTLAND A.S., *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, in *https://ieeexplore.ieee.org/document/7163223*/, 2015.
[343] Cfr. IBÁÑEZ, KIERON O'HARA L.D., SIMPERL E., *On Blockchains and the General Data Protection Regulation* cit., par. 6; SIMBULA M., *Dati personali: pull vs. push*,, in *https://studiolegalesimbula.com /dati-personali-pull-vs-push*/, 2017.
[344] Cfr., FINCK M., *Blockchains and Data Protection in the European Union*, *Max Planck Institute for Innovation & Competition Research Paper*, cit., pp. 17 ss.
[345] Cfr. RUSSO B., *L'evoluzione dei sistemi e dei servizi di pagamento nell'era digitale*, Padova, 2020, pp. 103 ss.

In particolare, il primo comma dell'art. 4, n. 1 del GDPR definisce il dato personale come qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente, su una *blockchain*, pubblica o privata. Il "Gruppo di lavoro articolo 29"[346] ha emanato linee guida su come devono essere interpretati i quattro elementi costitutivi – "qualsiasi informazione", "relativa a", "persona fisica" e "identificata o identificabile" – della nozione di dato personale: il termine "informazioni" deve essere inteso in senso ampio, così da includere sia informazioni oggettive (come i dati anagrafici o la presenza di una data sostanza nel sangue) sia analisi soggettive (come pareri e valutazioni), in qualsiasi forma (dati alfabetici o numerici, video e immagini); i dati possono essere considerati "relativi a" un soggetto quando si tratta di "quell'individuo", come, ad esempio, i dati relativi al veicolo che rivela informazioni su un dato soggetto come il conducente o il passeggero; un individuo è considerato "identificato" o "identificabile" quando può essere "distinto" dagli altri (non necessariamente attraverso il nome, ma anche con altri mezzi, come, ad esempio, il numero di telefono) e l'informazione, in ragione del suo contenuto, scopo o effetto, è collegata ad un particolare persona[347].

Il dato personale è assunto dal legislatore europeo, dunque, come un riflesso, una proiezione nella dimensione comunicativa, "capace di raffigurare l'individuo in maniera più o meno ampia, più o meno profonda, più o meno attuale e persino suscettibile di essere distaccata dalla persona cui si riferisce mediante le tecniche di pseudonimizzazione"[348].

Orbene, a tal proposito occorre menzionare l'art. 25 del GDPR, il quale individua un principio fondamentale in tema di trattamento dei dati nell'era digitale, ossia il principio di di *Privacy by Design* e *Privacy by Default*. La norma, in particolare, dispone: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del

[346] Il *Data Protection Working Party* - costituito in base all'art. 29 dir. 1995/46/CE - è stato di recente sostituito dallo *European Data Protection Board* (Comitato europeo per la protezione dei dati) come gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati.
[347] Parere 4/2007 del 20 giugno 2007, in *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1607426*.
[348] Cfr. PIRAINO F., *GDPR tra novità e discontinuità - I "diritti dell'interessato" nel Regolamento Generale sulla Protezione dei dati personali*, in *Giurisprudenza Italiana*, 2019, fasc. 12, p. 2777.

trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, 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. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica".

Così come improntato dal legislatore comunitario, dunque, il nuovo sistema delineato rappresenta un vero e proprio cambio di prospettiva nel modo di intendere la *privacy* e la protezione dei dati, atteso che agli operatori non è chiesto solamente di dare attuazione puntuale a tali disposizioni normative comunitarie, ma è richiesto, nello specifico, di dar vita ad un modello evolutivo, che, facendo perno sull'organizzazione e sulla tutela del dato, garantisca maggiore protezione al soggetto interessato dal relativo trattamento[349].

A differenza, dunque, di quanto accadeva in precedenza, nella quale non vi era un'integrazione di tale cultura nel tessuto organizzativo delle operazioni digitali, ma ci si limitava semplicemente ad istituire una unità organizzativa allo scopo destinata, limitandosi solamente ad effettuare dei controlli sul rispetto della normativa da parte delle istituzioni, oggi, invece, si richiede un approccio integrato di carattere sostanziale, in cui devono essere coinvolte tutte le aree di lavoro dell'organizzazione, in cui ogni singolo agente non si limita meramente ad adempiere alle prescrizioni normative, bensì dà luogo a comportamenti proattivi[350].

[349] GUZZO A., *Il Documento Programmatico sulla Sicurezza*, in *Lo Stato civile italiano*, 2010, fasc. 4, pp. 63-65.
[350] FIORENTINO L., *Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche*, cit., p. 690.

La tutela della *privacy*, allora, mediante il principio di *privacy by design* e *privacy by default* diventa parte integrante dei procedimenti digitali, diventa obiettivo cui ispirare ogni azione del soggetto pubblico e privato, atteso che, come abbiamo ampiamente illustrato in precedenza, tutte le attività che vengono compiute in rete, pongono in essere, producono e utilizzano dati in continuazione, in modo diretto e indiretto.

Al fine di consentire l'operatività dei principi individuati dalla disposizione in esame, in particolare, occorre che il titolare del trattamento ponga in essere tutte le politiche interne, nonché le misure interne ed organizzative necessarie. Il legislatore comunitario ha, infatti, espresso a chiare lettere che l'intento da raggiungere è la tutela dei dati sin dalla fase di sviluppo e progettazione. Di talché, nel momento in cui il Titolare si accinga a trattare i dati deve aver già individuato un sistema che ancor prima dell'avvio dell'attività di trattamento consideri le conseguenze e la portata del trattamento per l'interessato. Mediante questo meccanismo di valutazione *ex ante*, dunque, il titolare del trattamento sarà messo dinanzi al dovere di valutare se ridurre la portata del trattamento e l'ingerenza nella sfera dell'interessato, nonché, nella fase di creazione di prodotti e servizi nuovi, di valutare, sin dalla loro progettazione, le regole e i principi da rispettare in conformità a quanto previsto dal GDPR[351].

Ovviamente, la realizzazione di un tale sistema richiede, sin dal momento della determinazione dei mezzi del trattamento, di adottare misure tecniche e organizzative adeguate, quali anche la pseudonimizzazione e la minimizzazione dei dati, volte ad attuare in modo efficace i principi di protezione dei dati e ad integrare nel trattamento le garanzie necessarie a soddisfare i requisiti della normativa applicabile e tutelare i diritti degli interessati.

Dall'altro lato invece, il principio di *privacy by default* stabilisce che per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti tenendo in considerazione i principi

[351] FACCIOLI E., CASSARO M., *Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design*, cit., p. 561.

di non eccedenza e pertinenza. Pertanto potrà sicuramente essere utile, al fine di conformarsi a quanto stabilito dall'art. 25 del GDPR, ridurre al minimo il trattamento dei dati per utilizzare solo quelli strettamente necessari al perseguimento delle finalità individuate dal titolare, in virtù del c.d. "principio di minimizzazione"; adottare un periodo di conservazione dei dati, congruo rispetto al perseguimento delle finalità previste o a quello imposto da eventuali obblighi di legge prevalenti; dove possibile impostare un processo di pseudonimizzazione o implementare le cautele più stringenti possibili per ciascuno specifico trattamento; offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali; consentire all'interessato di controllare il trattamento dei dati (esercizio diritti degli interessati); ed infine consentire di creare e migliorare caratteristiche di sicurezza[352].

Incombe, dunque, sul Titolare del trattamento il dovere di definire il processo di *Privacy by design* e *By Default* al fine di garantire la protezione dei dati durante il processo di avvio di un nuovo trattamento, ovvero la minimizzazione dei dati personali oggetto di trattamento[353].

Da tali previsioni, dunque, emerge chiaramente come il trattamento del dato diviene questione centrale e intrinseca all'organizzazione stessa e al modo in cui si strutturano i processi, in linea con il valore e l'importanza che i dati stanno assumendo per l'economia, per le scelte pubbliche e per la lettura dell'intera società. Viene, dunque, richiesto mediante uno sforzo culturale e di formazione, di integrare il nuovo modello e di sfruttarne le potenzialità connesse ogniqualvolta venga in rilievo il trattamento dei dati[354].

---

[352] Cfr. PELLECCHIA E., *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove Leggi Civili Commentate*, 2020, fasc. 2, p. 360; VEALE M., BINNS R., AUSLOOS J., *When data protection by design and data subjects rights clash*, in *International Data Privacy Law*, 2018, pp. 105 ss.; GEORGE D., REUTIMANN K., TAMÒ-LARRIEUX A., *GDPR bypass by design? Transient processing of data under the GDPR*, in *International Data Privacy Law*, 2019, pp. 285 ss.

[353] Peraltro, in caso di inadempimento dell'obbligo di conduzione del processo per la gestione della protezione fin dalla progettazione, il Titolare del trattamento verrà considerato responsabile con conseguente comminazione della sanzione amministrativa pecuniaria prevista per tale violazione pari ad una somma fino ad Euro 10.000.000, o il 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

[354] FIORENTINO L., *Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche*, cit., p. 690.

3.2. (*Segue*) I dati personali utilizzati nella tecnologia *blockchain*.

Dopo aver definito cosa il GDPR intende per "dato personale", occorre, ora, procedere con l'analisi dei vari dati che possono essere immessi nell'ambito di una blockchain, per capire l'ambito di applicazione delle disposizioni regolamentari appena esaminate.

Anzitutto, è necessario prendere atto del fatto che in *blockchain* è ben possibile che vengano registrati una serie di dati che potrebbero rientrare nella definizione di dato personale così come delineata dal GDPR.

Invero, anzitutto, è possibile che siano inseriti documenti – come testi, immagini, audio, o altre tipologie – "in chiaro" contenenti dati personali. Si tratta senz'altro di un'ipotesi di utilizzo "anomalo" della *blockchain*, sia per i limiti di spazio sia per i costi associati ad un'operazione del genere, posto che tali documenti diverrebbero visibili a tutti i partecipanti del *network* e difficilmente potrebbero essere rimossi dal registro[355].

A questi occorre, poi, in secondo luogo, anche considerare quei dati registrati sulla *blockchain* associati alle transazioni, i c.d. "*metadati*" contenuti nell'*header* della transazione, necessari a identificarla ed a "legarla" alle precedenti. Insieme a questi dati alcune *blockchain*, come *Bitcoin*, consentono anche di inserire dei brevi testi – di circa 80 *bytes* – i quali saranno inclusi nella transazione e, quindi, registrati.

È anche possibile registrare informazioni (*file*) precedentemente cifrate. Con questa tecnica il *file* in chiaro rimarrà *off-chain* mentre l'*hash* dello stesso sarà registrato sulla *blockchain*, con la conseguenza che sarà ben possibile "tracciare" le transazioni relative al documento e verificare il momento in cui detto documento è stato inserito nel registro.

Le *blockchain*, infine, si basano sull'utilizzo da parte dei partecipanti di chiavi asimmetriche. Mentre la componente privata della chiave non è conosciuta

[355] Cfr. SARZANA DI S.IPPOLITO F., NICOTRA M., *Diritto alla blockchain, intelligenza artificiale e IOT*, cit., p. 76.

dai partecipanti al *network*, la chiave pubblica è conoscibile da tutti, e, tramite il *Public Key Hash*, costituisce l'identificativo destinatario delle transazioni.

Quelli appena descritti rappresentano i vari tipi di informazione che possono essere registrati all'interno di una *blockchain*. Qualora vengano registrati direttamente *file* in chiaro o siano contenuti dati personali negli *header* delle transazioni non vi sono dubbi circa il trattamento di tali dati da parte dei singoli nodi partecipanti.

È, necessario procedere, a questo punto, anzitutto a comprendere come operi l'anonimizzazione e la pseudoanonimizzazione in *blockchain*, per, poi, passare alla disamina, altresì, della disciplina delle informazioni che sono registrate previa cifratura (tramite la funzione di *hash*) e quella delle chiavi pubbliche.

3.3. (*Segue*) Anonimizzazione e pseudoanonimizzazione e chiavi pubbliche.

Il Considerando n. 26 del GDPR chiarisce che i principi della protezione dei dati personali non dovrebbero applicarsi a informazioni anonime, ossia a "informazioni che non si riferiscono a una persona identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".

Il *Working Party ex* art. 29 ha adottato, in data 10 aprile 2014, un apposito documento sulle tecniche di anonimizzazione, intitolato "*Opinion 05/2014 on Anonymisation Techniques*". Il processo di anonimizzazione[356] consiste nel trattare il dato in modo che non sia più possibile utilizzarlo per identificare una persona fisica, utilizzando tutti i mezzi che sia ragionevole aspettarsi, con l'importante precisazione che tale processo deve essere irreversibile[357]. Orbene, nella società

[356] La definizione di "dato anonimo" non è contenuta nel Regolamento europeo, ma nel Considerando n. 26, il quale recita: "I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".

[357] Le tecniche di anonimizzazione prese in considerazione dal WP29 sono due: la randomizzazione del dato, in cui si altera la veridicità del dato, al fine di rimuovere la connessione con la persona fisica; la seconda tecnica è la generalizzazione, che si ottiene diluendo le informazioni tramite ampliamento della scala di riferimento.

dell'informazione, in cui raccogliere dati o catalogare informazioni, operando collegamenti non prevedibili dagli interessati, è divenuta attività quotidiana e facilmente realizzabile, la qualificazione del dato come anonimo acquista un rilievo significativo. Come sottolineato in dottrina, "l'elemento chiave, che segna la distinzione tra dato personale e dato anonimo, è la collegabilità. La collegabilità dipende da numerosi fattori: dal soggetto che opera il collegamento, dal contesto nel quale esso opera e dal dominio di conoscenze che questi ha a sua disposizione"[358]. Ciò determina, dunque, la relatività del concetto di anonimato: si configura in relazione a determinati soggetti o a circostanze specifiche, caso per caso[359]. Con riferimento ai dati anonimi, il Regolamento non trova applicazione.

Diverso è il processo di pseudonimizzazione. Secondo il primo comma, n. 5 dell'art. 4 del GDPR tale processo consiste nel "trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

Da un punto di vista letterale, la disposizione si riferisce ad un metodo di trattamento piuttosto che ad una tipologia di dati: trattamento dei dati in modo tale che i dati possano essere attribuiti ad una persona interessata solo con l'aiuto di ulteriori informazioni. Non sono prescritti metodi precisi. La pseudonimizzazione non è un metodo di anonimizzazione: essa riduce la collegabilità di un *set* di dati con l'identità originaria di una persona interessata, ed è di conseguenza una misura di sicurezza utile. Pertanto, i dati pseudonimi sono ancora dati personali, ma il loro trattamento è considerato meno rischioso per le persone interessate[360].

---

[358] Cfr. FINOCCHIARO G., *Intelligenza artificiale e diritto - Intelligenza artificiale e protezione dei dati personali*, in *Giurisprudenza Italiana*, 2019, fasc. 7, p. 1657.

[359] Sul punto, in particolare, FINOCCHIARO G., *Diritto all'anonimato. Anonimato, nome, identità personale*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia*, Galgano (diretto da), Padova, 2008, passim.

[360] È fondamentale ricordare che, ai sensi del 30° considerando, le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (*cookies*) o a identificativi di altro tipo, come i *tag* di identificazione a radiofrequenza. Tali identificativi, pur essendo di carattere pseudonimo, possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle.

Sul punto, sempre il Considerando n. 26, precisa che i "dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. 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".

Il Considerando, con tutta probabilità fa riferimento ai principi elaborati dalla giurisprudenza della Corte di Giustizia dell'Unione Europea, nel caso C-582/14 *Patrick Breyer vs. Bundesrepublik Deutschland* del 19 ottobre 2016[361], in cui, con riferimento alla possibilità di inquadrare un indirizzo IP dinamico quale dato personale, i giudici hanno chiarito che tale deve considerarsi quel dato che appare ragionevolmente probabile che possa essere utilizzato per identificare una persona fisica, anche da una terza parte, a meno che l'identificazione della persona interessata sia proibita dalla legge o sia praticamente impossibile a causa del fatto che richiede uno sforzo sproporzionato in termini di tempo, costi e risorse, in modo che il rischio di identificazione appaia nella realtà essere insignificante.

Il GDPR incoraggia esplicitamente la pseudonimizzazione come misura di gestione del rischio. La pseudonimizzazione può essere considerata una prova del rispetto dell'obbligo di sicurezza del titolare del trattamento ai sensi dell'art. 5, lettera f) del GDPR, in linea con i principi basilari di *privacy by design* e *by default*[362].

Più nel dettaglio, la tecnica di pseudonimizzazione consiste nel sostituire un attributo con un altro, come, ad esempio, un dato anagrafico con un altro dato non

---

[361] Cfr. BERTI SUMAN A., *Indirizzi IP dinamici e cybersicurezza: la conservazione dei "dati personali" degli utenti da parte dell'Internet Provider nel caso Breyer*, in *Orientamenti della Corte di Giustizia dell'Unione Europea in materia di responsabilità civile*, di Alpa G., Conte G., (a cura) Miilano, 2018, pp. 119 ss.

[362] Cfr. PIZZETTI F., *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 116.

direttamente identificativo, mantenendo il collegamento in un contenitore separato. Il soggetto rimane identificabile, mentre il dato pseudonimizzato da solo non è idoneo a tale scopo.

Tra le tecniche di pseudonimizzazione indicate dal WP29 vi è anche la funzione di *hash*, che è considerata tale in quanto conoscendo l'intervallo di valori si potrebbero creare una serie di *output*, attraverso la medesima funzione di *hash*, per ricavare quello corretto.

Tale inquadramento da parte del WP29, in uno con le definizioni e considerazioni sopra riportate contenute nel GDPR, portano necessariamente a considerare i dati registrati su *blockchain*, anche se cifrati tramite applicazione di una funzione di *hash*, come dati personali[363] con conseguente applicazione delle regole stabilite dal Regolamento europeo. Tale conclusione è oramai avvalorata anche dalla Risoluzione del Parlamento UE P8_TA-PROV(2018)0373, che al considerando D espressamente considera come elemento delle *Distributed Ledger Technology*, la pseudonimizzazione degli utenti, e non la loro anonimizzazione, sottolineando al punto 33 "che è della massima importanza che gli usi della DLT siano conformi alla legislazione dell'UE sulla protezione dei dati, in particolare al regolamento generale sulla protezione dei dati (GDPR)" nel contempo invitando la Commissione ed il Garante europeo della protezione dei dati (GEPD) a fornire ulteriori orientamenti su questo punto.

Simili considerazioni, con alcune distinzioni, possono svolgersi anche con riferimento alle chiavi pubbliche registrate sulla *blockchain*.

Parte della dottrina[364] ritiene che le chiavi pubbliche siano comunque dei dati personali pseudonimizzati, ciò in quanto non potrebbero considerati anonimizzati, non soddisfacendo il requisito dell'irreversibilità del processo. Altri

---

[363] Cfr. IBÁÑEZ, KIERON O'HARA L.D., SIMPERL E., *On Blockchains and the General Data Protection Regulation* cit., par. 4; FINCK M., *Blockchains and Data Protection in the European Union*, *Max Planck Institute for Innovation & Competition Research Paper*, cit., p. 23; NICOTRA M., *Blockchain e GDPR: le norme da conoscere per tutti i problemi*, cit.. Cfr., altresì, la Risoluzione del parlamento UE del 3 ottobre 2018, in *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NON SGML+TA+P8-TA -2018-0373+0+DOC+PDF+V0//IT*.

[364] Cfr. FINCK M., *Blockchains and Data Protection in the European Union*, *Max Planck Institute for Innovation & Competition Research Paper*, cit., p. 24.

Autori[365], invece, escludono la possibilità di considerarle dati personali fin quando l'utente della *blockchain* mantiene segreta la componente privata delle stesse e sulla base di quanto previsto nel Considerando n. 26 (che riprende i principi dettati dalla Corte di Giustizia relativi ai fattori obiettivi, quali il tempo, il costo e le risorse da impiegare, da valutare per comprendere se un dato pseudonimizzato possa essere considerato anonimo), precisando però che nel momento in cui, in una *blockchain permissionless*, tali chiavi vengano associate da parte dei *Blockchain Service Provider* a delle persone fisiche esse devono connotarsi come dati personali per l'analogia che viene a crearsi con il caso esaminato dalla Corte stessa.

Il punto è che tutte le operazioni effettuate all'interno del sistema sono registrate e archiviate nella *blockchain* (ciascuna con una propria marcatura temporale), e restano liberamente consultabili, per un periodo di tempo illimitato, da qualunque soggetto, anche se questi non partecipa alla rete. La pseudonimia protegge solo parzialmente l'identità degli utilizzatori: infatti, la *blockchain* non include informazioni che consentono di risalire (direttamente) alla persona che ha effettuato il trasferimento, ma soltanto alla sua chiave pubblica[366]. Si è però da più parti evidenziato che un tale mascheramento non esclude la possibilità di ricavare, attraverso un incrocio dei dati contenuti nella *blockchain* unitamente alle tracce lasciate sul *web* dal soggetto che ha concretamente disposto le operazioni, la reale identità dell'individuo cui è riconducibile la chiave pubblica e, quindi, tutte le transazioni che lo hanno riguardato[367].

Non può comunque sottacersi il fatto che, in verità, sono state già poste in essere delle tecniche per risalire all'identità degli utilizzatori di una *blockchain* attraverso l'analisi grafica delle transazioni. Inoltre, non è inusuale che un soggetto dichiari la propria chiave pubblica per ricevere dei fondi e stanno già nascendo servizi professionali volti proprio ad identificare le persone che operano sulle *blockchain*[368]. Anche l'analisi di altri dati di contesto, come gli indirizzi IP da cui

---

[365] Cfr. IBÁÑEZ, KIERON O'HARA L.D., SIMPERL E., *On Blockchains and the General Data Protection Regulation* cit., par. 4.
[366] Cfr. FRANCO P., *Understanding Bitcoin*, *Understanding Bitcoin. Cryptoghraphy*, *Enginnering and Economics*, cit., pp. 209 ss.
[367] Cfr. EENMAA-DIMITRIEVA H., SCHMIDT-KESSEN M.J., *Regulation Through Code as a safeguard for implementing smart contracts in no-trust environments*, cit., pp. 17-19.
[368] Cfr. *https://www.chainalysis.com/*.

ci si collega al *network* o un insieme di transazioni che riportano più chiavi pubbliche, consentono di risalire ad un utente specifico[369]. Infine, nel caso di *blockchain* che consentono lo sviluppo di *smart contract* non può escludersi che l'esecuzione degli stessi richieda il trattamento di dati personali, anche ulteriori rispetto alle chiavi pubbliche associate a persone fisiche.

Ben si comprende, dunque, perché in *Bitcoin*, così come in tutti gli altri strumenti tecnologici basati sul concetto di *blockchain*, sussista una tensione fondamentale tra le esigenze postulate dalla tracciabilità delle operazioni e la riservatezza dei suoi utilizzatori. Come si è detto, infatti, il funzionamento del sistema è reso possibile dall'esistenza di un registro pubblico, perpetuo e immodificabile, contenente tutte le transazioni avvenute. È evidente che questo limite costituisce un *vulnus* non trascurabile nei confronti della tutela della *privacy*, visto il carattere personale e la rilevanza delle informazioni che possono essere contenute all'interno della *blockchain*, specialmente nel caso in cui tali dati non si riferiscano (soltanto) a trasferimenti di fondi[370].

Stante la potenziale riconducibilità ad una persona fisica determinata delle informazioni registrate sulla *blockchain* appare più corretto concludere per l'applicabilità del GDPR ai dati registrati su *blockchain*, quali dati pseudonimizzati, così essendo necessario, in relazione alle diverse fattispecie che di volta in volta vengono in rilievo, esaminare l'applicabilità del Regolamento Europeo a tale particolare tecnologia. Va da sé, infatti, che l'applicazione di tali disposizioni normative presenterà problematiche di non poco rilievo nei confronti dei sistemi *blockchain*, i quali trovano nell'immutabilità delle informazioni contenute al loro interno la migliore garanzia della propria sicurezza e affidabilità. Né può valere ad escludere le tecnologie *blockchain* dal campo di applicazione del Regolamento la considerazione per cui i dati vengono conservati in forma pseudonima: infatti, il GDPR estende l'applicabilità delle disposizioni in materia di protezione dei dati personali anche alle informazioni pseudonimizzate, in quanto

[369] Una delle tecniche per evitare di essere identificati, suggerita dallo stesso Satoshi Nakamoto, è quella di creare nuove coppie di chiavi per ogni transazione. Tale tecnica però, oltre a non essere agevole da utilizzare, comporta comunque il passaggio delle criptovalute da una chiave pubblica ad un'altra, così consentendo di risalire la catena per individuare il titolare delle stesse

[370] Cfr. RINALDI G., *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 257.

tale accorgimento non è sufficiente a impedire in radice l'identificabilità dell'individuo a cui si riferiscono le informazioni "mascherate"[371].

4. Elementi di criticità tra la *blockchain* ed il GDPR.

La prima considerazione da fare nella disamina specifica dei rapporti tra *blockchain* e GDPR è che la *blockchain* contrasta con la *Data Protection* su due aspetti che, a ben guardare, rappresentano gli elementi fondanti della tecnologia in commento: anzitutto, la pubblicità dei dati: quelli inseriti nelle *blockchain* sono pubblici e accessibili da chiunque partecipi alla catena; in secondo luogo, la loro durata temporale: essi infatti sono conservati illimitatamente a tutela dell'intero registro distribuito. Si tratta di elementi che insieme consentono di creare un archivio "decentralizzato" ed immutabile.

Il maggior attrito concerne proprio il fatto che l'applicabilità delle disposizioni contenute nel Regolamento *privacy* riguardano principalmente la constatazione che esso nasce con il fine di disciplinare i già menzionati "*data silos*", ossia i casi di trattamento "centralizzato" di dati personali; mentre la tecnologia *blockchain* si basa fondamentalmente sulla "decentralizzazione" e distribuzione delle operazioni di computo su un *network*.

Di talché si rivela operazione alquanto difficoltosa quella di provare a conciliare i profili decisamente privatistici della *Data Protection* con un sistema di blocchi all'interno del quale confluiscono enormi quantità di dati e informazioni, non più cancellabili né modificabili. Ciò, infatti, già solo ad un primo impatto – che approfondiremo nel prosieguo della trattazione – si rivela del tutto confliggente con quanto stabilito all'art. 17 del Regolamento secondo cui l'interessato ha diritto ad ottenere la cancellazione dei propri dati personali quando la finalità per cui sono stati raccolti è venuta meno; in altre parole, quando è stato revocato il consenso che ne autorizza il trattamento e in una serie di altri casi (c.d. "diritto all'oblio" o "*right to be forgotten*").

[371] Cfr. RINALDI G., *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 257.

4.1. (*Segue*) L'operatività dei principi del GDPR nell'ambito della tecnologia *blockchain*.

Il carattere distribuito ed aperto della *blockchain*, nonché le sue caratteristiche di immutabilità, suscitano complicanze anche rispetto all'esercizio di taluni dei diritti riconosciuti dal GDPR agli interessati.

4.1.1. (*Segue*) Il principio di esattezza e di rettifica nel trattamento dei dati personali.

In particolare, il primo comma dell'art. 5, lettera d) GDPR prevede il c.d. principio di "esattezza" dei dati, in virtù del quale le informazioni trattate devono essere esatte e, se necessario, aggiornate. Inoltre, devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente quei dati che risultino inesatti rispetto alle finalità per le quali sono trattati, diritto espressamente regolato dall'art. 16 del Regolamento[372].

Più nel dettaglio, l'art. 16 del Regolamento attribuisce all'interessato il diritto di conseguire dal titolare, senza ingiustificato ritardo e in ogni caso entro un mese dal ricevimento della richiesta – ai sensi del paragrafo dell'art. 12 del Regolamento –, la rettifica dei propri dati personali inesatti, ma anche l'integrazione di quelli incompleti alla luce della finalità del trattamento, anche mediante il rilascio di una dichiarazione integrativa[373].

La dottrina, in particolare, ha proposto di annoverare tale posizione sostanziale tra quelle di "natura dinamica", che attribuiscono all'interessato poteri e facoltà di intervento sul trattamento dei dati personali che lo riguardino[374].

Il c.d. diritto di rettifica va considerato come un nucleo di prerogative di natura strumentale che comporta l'eliminazione di inesattezze, il completamento di

---

[372] Sul punto cfr. LUCCHINI GUASTALLA E., *Privacy e data protection: principi generali*, in Tosi (a cura di), *Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, pp. 66 ss.; DELL'UTRI M., *Principi generali e condizioni di liceità del trattamento dei dati personali*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 179 ss.

[373] Cfr. CALISAI F., *I diritti dell'interessato*, cit., pp. 344 ss.; MONTANARO D., *Il diritto di accesso ai dati personali e il diritto di rettifica*, cit., pp. 195 ss.; RICCI A., *I diritti dell'interessato*, cit., pp. 189 ss.

[374] Cfr. CALISAI F., *I diritti dell'interessato*, cit., p. 344.

informazioni che risultino essere solamente parziali o il suo aggiornamento finalizzati sia ad ottenere maggiori vantaggi dal trattamento dei dati personali in essere, sia a perseguire l'obiettivo di una più fedele rappresentazione sociale di sé stessi. Facendo rientrare tali prerogative nell'ambito dei c.d. diritti dell'interessato, il legislatore pare aver voluto aderire a quell'idea dottrinaria secondo cui i c.d. diritti dell'interessato altro non siano che diritti su diritti[375].

La dottrina ha anche ricondotto il diritto di rettifica nell'ambito di quella categoria di diritti riconosciuti con la formula di "diritto all'identità personale", inteso come diritto della persona di nuova generazione che soppiantando il tradizionale concetto statico di identità, ancorato alle informazioni fissate nei registri dello stato civile, lo apre ora, come sottolineato dalla giurisprudenza, ad una "dimensione dinamica"[376] del processo: quello della costruzione della raffigurazione della propria persona nella dimensione pubblica dei rapporti sociali[377].

Orbene, come può evincersi da quanto descritto, può facilmente intuirsi che si tratti, però, di un diritto difficilmente esercitabile nell'ambito di una *blockchain* pubblica, sia in quanto il dato inesatto eventualmente registrato sulla stessa è conservato su tutti i nodi del *network* (e, quindi, l'interessato dovrebbe rivolgersi ad ognuno di essi), sia per la caratteristica tecnica di potenziale immutabilità dei dati registrati[378].

Una rettifica potrebbe essere effettuata tramite una "dichiarazione integrativa" (come previsto dall'art. 16 GDPR), senza cancellare i dati originari. Tale soluzione, pur se tecnicamente fattibile, richiederebbe una verifica in termini di compatibilità con la previsione normativa, ponendosi in una condizione che

---

[375] Cfr. CASTRONOVO C., *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*,, cit., p. 653.

[376] Di proiezione dinamica dei dati personali parla Corte di Cassazione, sentenza del 4 aprile 2012, n. 5525, in *Foro Italiano*, 2013, fasc. I, pp. 305 ss.: "Posta la necessaria rispondenza del trattamento dei dati personali ai criteri di proporzionalità, necessità, pertinenza e non eccedenza allo scopo, spetta all'interessato al trattamento, a tutela della proiezione dinamica dei suoi dati personali e della sua attuale identità personale o morale, il diritto di conoscere in ogni momento chi possiede i dati e le relative modalità di utilizzo con la possibilità di opporsi al trattamento degli stessi ovvero di chiederne la cancellazione, la trasformazione, il blocco, la rettifica, l'aggiornamento o l'integrazione"

[377] Cfr. RESTA G., ALPA G., *Le persone fisiche e i diritti della personalità*, Milano, 2019, pp. 480 ss.

[378] Per ottenere una modifica delle informazioni già registrate in un blocco sarebbe necessario raggiungere il consenso del 51% dei partecipanti al *network.*

rimanda alla mente il vecchio mondo analogico, nel quale non era possibile rettificare un dato in un registro cartaceo se non pubblicando una nuova informazione, senza però cancellare quella errata[379].

4.1.2. (*Segue*) Il diritto di accesso.

Anche il diritto di accesso e di ottenere copia dei dati personali, disciplinato dall'art. 15 GDPR, potrebbe essere di non semplice applicazione nell'ambito di una *blockchain*. In particolare, il diritto di accesso consiste in una posizione sostanziale che consente all'interessato di ricevere dal titolare, in primo luogo, la conferma dello svolgimento o meno di un trattamento dei propri dati personali e di accedere a questi ultimi mediante rilascio, senza spese, di una copia[380] e, poi, anche una serie di informazioni riproduttive di quelle prescritte dagli articoli 13 e 14 del Regolamento già in sede di ottenimento dei dati o entro un lasso di tempo ragionevole[381].

Il diritto di accesso consiste, dunque, nella facoltà dell'interessato di ottenere non una generica conferma, ma un riscontro circostanziato dell'esistenza di un trattamento di dati personali sul proprio conto. E, infatti, il primo paragrafo dell'art. 15 accorda all'interessato la pretesa di ottenere nuovamente – o per la prima volta nel caso di trattamenti intrapresi prima dell'entrata in vigore della normativa – informazioni relative alle caratteristiche dei dati e del trattamento, con particolare riferimento alle garanzie previste dall'art. 46, Regolamento nel caso in cui sia previsto il trasferimento dei dati a un Paese terzo o a un'organizzazione

[379] Cfr. SARZANA DI S.IPPOLITO F., NICOTRA M., *Diritto alla blockchain, intelligenza artificiale e IOT*, cit., p. 76.
[380] Cfr. ABETI R., *L'accesso ai dati personali*, in Cendon (a cura di), *Trattato dei nuovi danni*, II, *Malpractice medica, prerogative della persona, voci emergenti della responsabilità*, Padova, 2011, pp. 217 ss.
[381] Con riferimento al GDPR, cfr. CALISAI F., *I diritti dell'interessato*, cit., pp. 338 ss.; MONTANARO D., *Il diritto di accesso ai dati personali e il diritto di rettifica*, cit., pp. 185 ss.; RICCI A., *I diritti dell'interessato*, cit., pp. 182 ss.

internazionale[382], nonché ai "diritti" riconosciuti all'interessato dall'ordinamento[383].

Nel contenuto del diritto di accesso è inclusa la facoltà di acquisire una copia dei dati personali, al punto che in dottrina si suggerisce che la ricezione di copia dei dati rappresenti il risultato ultimo di tale diritto[384]. Tale prospettiva teleologica del diritto di accesso può essere limitata soltanto in presenza della correlativa lesione di diritti e di libertà altrui, di cui al paragrafo 4 dell'art. 15, del Regolamento[385].

Il diritto va esercitato mediante una richiesta indirizzata al titolare del trattamento, il quale deve dare riscontro senza giustificato ritardo e, in ogni caso, entro un mese dal ricevimento della richiesta, non potendosi dunque attribuire all'eventuale silenzio da parte del titolare nessun altro valore giuridico che quello dell'inadempimento dell'obbligo di comunicazione correlato al diritto di accesso[386].

Il riconoscimento della facoltà di ricevere copia dei dati rappresenta una novità del Regolamento rispetto alla normativa italiana previgente, nella quale tale prerogativa non era in alcun modo espressamente riconosciuta così che la si riteneva sussistente soltanto in termini strumentali, quando il rilascio della copia dei dati si rivelava necessario per soddisfare il diritto di accesso e, dunque, per portare a conoscenza dell'interessato quali suoi dati fossero oggetto di trattamento[387].

---

[382] Sul punto cfr. PIRODDI P., *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, in *Diritto dell'Informatica*, 2015, pp. 827 ss. e, con riferimento al GDPR, RICCIO G.M., PEZZA F., *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*, in Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, pp. 585 ss.

[383] Le informazioni incluse nel diritto di accesso di cui all'art. 15, Regolamento sono: "a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, parr. 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato".

[384] Cfr. CALISAI F., *I diritti dell'interessato*, cit., pp. 338.

[385] Per il rapporto tra diritto di accesso agli atti amministrativi e diritto alla riservatezza e protezione dei dati personali cfr. CALISAI F., *I diritti dell'interessato*, cit., pp. 339-340.

[386] Come sottolineato da CALISAI F., *I diritti dell'interessato*, cit., pp. 341, va esclusa l'ammissibilità del silenzio-rifiuto.

[387] Cfr. Garante privacy 12 giugno 2000, XY/INAIL; Garante privacy 20 marzo 2002, Marzano/Banco di Napoli s.p.a.; Garante privacy, 9 maggio 2002, XY/Sara Assicurazioni s.p.a.

Orbene, riportando ora quanto detto nell'ambito delle *Distributed Ledger Technology*, è stato evidenziato dalla dottrina[388] che seppur in una *blockchain permissionless* l'interessato potrebbe aderire al *network* ottenendo così copia di tutta la *blockchain* e dei dati in essa conservati, difficilmente potrà consultarli se registrati in maniera cifrata e pseudonimizzata. La copia della *blockchain* così ottenuta potrebbe, quindi, non corrispondere alle informazioni riferibili all'interessato trattate da alcuni dei partecipanti al *network*, che egli dovrebbe riuscire ad individuare e richiedere singolarmente ad ognuno di essi[389].

4.1.3. (*Segue*) Il diritto alla cancellazione ed il diritto all'oblio.

Il Regolamento *Data protection* ha riservato particolare attenzione al c.d. diritto alla cancellazione[390] in quanto mezzo per l'esercizio del diritto all'oblio dell'interessato[391].

In questo caso, la dottrina ha ritenuto che più che parlare di una posizione sostantiva, sarebbe più opportuno ritenere che quello introdotto dal legislatore sia un rimedio, come la strumentalità al diritto all'oblio parrebbe confermare[392].

La cancellazione si connota, tuttavia, per avere un contenuto più ampio, rappresentandosi, non solo come il potere di riappropriarsi delle informazioni di carattere personale nel caso tanto di trattamento illecito o scorretto, come disposto dal primo paragrafo, lettera d) dell'art. 17 del Regolamento, ma anche come obbligo

---

[388] Cfr. FINCK M., *Blockchains and Data Protection in the European Union*, *Max Planck Institute for Innovation & Competition Research Paper*, cit., p. 30.
[389] Cfr. SARZANA DI S.IPPOLITO F., NICOTRA M., *Diritto alla blockchain, intelligenza artificiale e IOT*, cit., p. 76.
[390] Sul punto cfr. DI CIOMMO F., *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, cit., pp. 358 ss.; BERTI SUMAN A., *Il diritto alla cancellazione*, cit., pp. 199 ss.; RICCI A., *I diritti dell'interessato*, cit., pp. 195 ss.
[391] Cfr. RESTA G., ZENO-ZENCOVICH V. (a cura di), I*l diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015, passim; PIZZETTI F. (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, passim; FERRI G.B., *Diritto all'informazione e diritto all'oblio*, cit., pp. 801 ss.; MORELLI M.R., *Oblio (diritto all')*, in *Enciclopedia del Diritto*, Agg. VI, Milano, 2002, pp. 848 ss.; MEZZANOTTE M., *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009, pp. 81 ss., 199 ss., 151 ss. Con riferimento al GDPR, cfr. DI CIOMMO F., *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, cit., pp. 371 ss.; SAMMARCO P., *Privacy digitale, motori di ricerca e social network: dal diritto di accesso e rettifica al diritto all'oblio condizionato*, cit., pp. 166 ss.; RICCI A., *I diritti dell'interessato*, cit., pp. 201 ss.
[392] Cfr. PIRAINO F., *GDPR tra novità e discontinuità - I "diritti dell'interessato" nel Regolamento Generale sulla Protezione dei dati personali*, cit., p. 2777.

legale di cancellazione imposto al titolare dal diritto dell'Unione europea o dello Stato membro di appartenenza, e come, infine, esercizio di un potere sostanziale di "autodeterminazione informativa"[393].

La cancellazione dei dati personali può essere richiesta, infatti, anche in presenza di un trattamento lecito e corretto in conseguenza della scelta libera e consapevole dell'interessato di interrompere il trattamento dei propri dati personali in ordine a una o più finalità determinate, qualora l'impiego e la circolazione di tali informazioni non vengano più reputati opportuni o comunque non risultino più graditi o ancora confliggano con gli obiettivi e le strategie dell'interessato in ordine alla costruzione o all'evoluzione della propria identità personale o anche soltanto con più limitati fini specifici[394].

Questa è la *ratio* sulla quale l'art. 17 del GDPR fonda il diritto alla cancellazione: a seguito di revoca del consenso da parte dell'interessato[395], a meno che il trattamento non poggi anche su un'altra base giuridica che ne giustifichi la prosecuzione – lettera b) – ; in conseguenza dell'opposizione al trattamento di cui

---

[393] Cfr. THIENE A., *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, Ferrara, 2017, pp. 425 ss.

[394] Sostenitori dell'impostazione tradizionale del concetto di identità personale come nozione statica, cfr. FALCO G., voce *Identità personale*, in *Nuovo Digesto Italiano*, VI, Torino, 1938, p. 649; ZENO-ZENCOVICH V., voce *Identità personale*, in *Digesto delle Discipline Civilistiche*, IX, Torino, 1993, pp. 294 ss. Sull'evoluzione del concetto di identità personale da nozione statica, sostanzialmente coincidente col nome e con gli altri segni identificativi rilevati ai fini dello stato civile, a categoria relazionale dinamica, ossia come processo, frutto di personale elaborazione e coincidente con la rappresentazione esterna della propria personalità cfr. PINO G., *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003, pp. 181 ss.; PINO G., *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in *Libera circolazione e protezione dei dati personali*, I, Milano, 2006, pp. 259 ss.; PINO G., *L'identità personale*, in *Trattato di biodiritto*, diretto da Rodotà S., Zatti P., *Ambito e fonti del biodiritto*, a cura di Rodotà, Tallacchini, Milano, 2010, pp. 297 ss.; RESTA G., *Identità personale e identità digitale*, in *Diritto dell'Informatica*, 2007, pp. 511 ss. in part. p. 521; RESTA G., *Dignità, persone, mercati*, Torino, 2014, pp. 323; ZATTI P., *Dimensioni ed aspetti dell'identità nel diritto privato attuale*, in *Nuova Giurisprudenza Commentata*, 2007, suppl., pp. 1 ss.; FINOCCHIARO G., *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Diritto dell'Informatica*, 2012, pp. 383 ss.; PASQUINO T., *Identità digitale della persona, diritto all'immagine e reputazione*, in Tosi (a cura di), *Privacy digitale*, Milano, 2019, pp. 93 ss.; FUSARO A., *Nome e identità personale degli enti collettivi. Dal "diritto" all'identità uti singuli al "diritto" all'identità uti universi*, in *Nuova Giurisprudenza Commentata*, 2002, fasc. II, pp. 51 ss.

[395] Il tema della revoca del consenso ha accesso un vivace dibattito dottrinale: cfr. MAZZAMUTO S., *Il principio del consenso e il problema della revoca*, in *Libera circolazione e protezione dei dati personali*, I, Milano, 2006, pp. 993 ss.; FICI A., PELLECCHIA E., *Il consenso al trattamento*, in *Diritto alla riservatezza e circolazione dei dati personali*, I, Milano, 2003, pp. 469 ss.; RESTA G., *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Rivista Critica di Diritto Privato*, 2000, pp. 299 ss.; THOBANI S., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Genova, 2018, pp. 147 ss.

all'art. 21, Regolamento, a meno che non prevalga l'interesse legittimo del titolare alla prosecuzione – lettera c) –; in caso di trattamento di dati personali raccolti nell'ambito dell'offerta diretta di servizi della società dell'informazione ai minori che abbiano compiuto almeno sedici anni, ai sensi dell'art. 8, primo paragrafo, del Regolamento – lettera f) –[396].

La cancellazione dei dati resi pubblici dal titolare implica anche l'adozione delle misure ragionevoli e proporzionate[397], anche di natura tecnica, necessarie a informare gli ulteriori titolari che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali, a norma dell'art. 17, secondo paragrafo, del Regolamento.

Orbene, la caratteristica di "immutabilità" di una *blockchain* può far ritenere che tale tecnologia non consenta il puntuale rispetto del diritto alla cancellazione e del diritto all'oblio, nei termini sanciti dal GDPR a tutti gli interessati, intesi, cioè come l'obbligo del titolare, qualora abbia comunicato i dati a terzi, di cancellarli ed informare gli altri titolari della richiesta dell'interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali[398].

Invero, il primo passo è quello di comprendere se effettivamente l'interessato che abbia utilizzato un servizio basato su *blockchain* possa esercitare il diritto alla cancellazione sulla base di uno dei motivi indicati dalle lettere a) ad f) del primo comma dell'art. 17 GDPR. Ogni dato inserito in una *blockchain*, infatti,

---

[396] La cancellazione non può essere disposta qualora il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'art. 9, par. 2, lett. h) e i), e dell'art. 9, par. 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'art. 89, par. 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria (art. 17, par. 3, Regolamento).

[397] Sottolinea il ruolo assunto nella disciplina sulla protezione dei dati personali da concetti normativi indeterminati come quello di ragionevolezza FINOCCHIARO G., *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Le nuove leggi civili commentate*, 1/2017, p. 16. Sul concetto di ragionevolezza nel diritto civile cfr. PIRAINO F., *Per una teoria della ragionevolezza in diritto civile*, in *Europa e Diritto Privato*, 2014, pp. 1287 ss.; PIRAINO F., *Buona fede, ragionevolezza e "efficacia immediata" dei principî*, Napoli, 2017, pp. 33 ss. Contra PERLINGIERI G., *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, pp. 45 ss.

[398] Cfr. SARZANA DI S.IPPOLITO F., NICOTRA M., *Diritto alla blockchain, intelligenza artificiale e IOT*, cit., p. 76.

risulta indispensabile per mantenere la "catena" di transazioni relative alla medesima "informazione digitale", funzione che caratterizza la *blockchain* rispetto alle altre tecnologie. Peraltro, se consideriamo che sia la chiave pubblica sia l'*hash* delle transazioni sono riconducibili – come suggerito anche dall'*Opinion WP29* –, alla categoria dei dati pseudonimizzati, sarebbe astrattamente possibile esercitare il diritto alla cancellazione nei confronti del soggetto che detiene la porzione di dato che consente l'identificazione dell'interessato.

Se ci si affida al dato letterale, in verità, il diritto all'oblio contiene già nella sua previsione normativa una precisazione e limitazione idonea a ridimensionarne la sua portata, considerato che la norma regolamentare precisa che esso deve essere esercitato "tenendo conto della tecnologia disponibile e dei costi di attuazione".

Si tratta, dunque, di comprendere se il riferimento alla "tecnologia disponibile" possa essere sufficiente, stante le caratteristiche della *blockchain*, ad escludere l'applicazione del diritto all'oblio in considerazione proprio dei suoi limiti tecnologici optando, eventualmente, per soluzioni alternative[399], non dimenticando, peraltro, che anche il Parlamento europeo, nella Risoluzione del 3 ottobre 2018, ha espressamente riconosciuto che "il diritto all'oblio non è facilmente applicabile in questa tecnologia".

La dottrina, inoltre, non ha mancato di rilevare che, a ben vedere, il GDPR non definisce cosa debba intendersi per cancellazione e a ciò va anche aggiunta la considerazione per cui alcune normative nazionali, come, ad esempio, quella tedesca, prevedono che qualora le specifiche modalità di conservazione non consentano la cancellazione del dato è previsto che sia sufficiente limitarne l'utilizzo, rendendolo inaccessibile[400].

Lo stesso discorso vale anche con riferimento al principio di *privacy by design* previsto dall'art. 25 del Regolamento, riassumibile, come abbiamo già visto, nella necessità che i trattamenti, sia nel momento della progettazione dei sistemi sia

[399] Tra cui procedure formalizzate di consegna o cancellazione delle chiavi privati, che rendono inaccessibili i dati cifrati. Cfr. FINCK M., *Blockchains and Data Protection in the European Union*, *Max Planck Institute for Innovation & Competition Research Paper*, cit., p. 30.; DE FILIPPI P., *The interplay between decentralization and privacy: the case of blockchain technologies*, in *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689*, 2016.

[400] Cfr. FINCK M., *Blockchains and Data Protection in the European Union*, *Max Planck Institute for Innovation & Competition Research Paper*, cit., p. 30.

in occasione del loro uso, vengano effettuati nel rispetto delle previsioni e dei principi del Regolamento. Orbene, tale disposizione contiene un *incipit* secondo cui tale obbligo deve essere attuato "tenendo conto dello stato dell'arte e dei costi di attuazione", nonché "della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento", enunciando, dunque, le tecniche di minimizzazione e pseudonimizzazione dei dati personali come strumenti per ottenere l'obiettivo del rispetto dei principi dettati dal GDPR nella realizzazione ed utilizzo dei sistemi ed applicazioni. Il punto è che, nella maggior parte dei casi, i dati sulle *blockchain* sono registrati proprio in forma pseudonimizzata, mentre la minimizzazione potrebbe essere ottenuta tramite la registrazione *off-chain* delle informazioni personali degli interessati.

5. Alcune potenzialità della *blockchain* a vantaggio della protezione dei dati personali.

Dopo aver sottolineato le criticità inerenti la tecnologia *blockchain* e le disposizioni sulla tutela della privacy introdotte dal *Data Protection*, passiamo ora a vedere quali sono, invece, le potenzialità della tecnologia in commento rispetto alla protezione dei dati personali.

Invero, guardando l'argomento in esame da un'altra angolazione, attraverso la *blockchain* un utente è sempre in grado di controllare i propri dati personali, anzi, è l'unico a sapere a quali informazioni corrisponde la propria chiave pubblica, secondo un principio di "disaccoppiamento" dei dati dall'entità individuale per essere attribuito ad uno pseudonimo[401]. Questo consente di tracciare lungo tutta la catena distribuita dove e come sono usate le informazioni oggetto di una

[401] Solitamente la chiave è cifrata di modo che dalla singola transazione non è possibile risalire a colui che è titolare di detta chiave, ma l'eventuale riutilizzo di quest'ultima in altre transazioni (anche in congiunzione con altre chiavi pubbliche) consentirebbe di "linkarla" ad un utente specifico potendo quindi risalire alla sua identità. Oltretutto, l'eventuale disponibilità di log di accesso con conservazione di indirizzi IP renderebbe facilmente individuabile il titolare della chiave pubblica della transazione.

transazione: ogni dato inserito in una *blockchain* è necessario per mantenere la "catena" di transazioni relative alla medesima "informazione digitale", caratterizzando nello specifico siffatta tecnologia rispetto alle altre.

Vista dalla prospettiva della protezione dei dati personali degli utenti, la tecnologia *blockchain* adotta sicuramente un approccio *privacy by design* secondo quanto stabilito dall'art. 25 del Regolamento – mediante il quale, come abbiamo detto, si riducono al minimo l'elaborazione e la confidenzialità dei dati fin dalla progettazione del sistema di trattamento – puntando sui suoi aspetti di maggiore forza, ossia le tecniche della crittografia e della pseudonimizzazione[402], elemento di grande novità rispetto al precedente *Codice Privacy*.

In particolare quest'ultima tecnica consiste nel disaccoppiare i dati dall'identità individuale attraverso uno schema del tutto simile a quello contenuto nella funzione di *hash* utilizzata dalla *blockchain*[403], rendendo di fatto applicabile il GDPR[404]: l'*hashing* infatti è una tecnica di pseudonimizzazione – e non di anonimizzazione – idonea a registrare dati personali riferiti ad individui

---

[402] Se ne ha contezza nell'ambito dello stesso art. 32 del Regolamento *Data Protection*, il quale prevedere tali misure come adeguate a garantire la sicurezza del trattamento dai dati personali. Mentre l'art. 4, primo comma, n. 5 definisce la tecnica di pseudonimizzazione come "il trattamento di dati personali in modo tale che [...] non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".
Si veda anche, Raccomandazione n.3/97, *Anonymity on Internet* (WP6), dell'*Article 29 Working Party*, e Parere n. 5/2014, *Anonymisation Techniques* (WP216).
L'introduzione del concetto di pseudonimizzazione rappresenta una significativa opportunità per le imprese in quanto consente di definire nuove strategie e modelli di *business* basati sull'analisi/correlazione della grande mole di dati disponibili in azienda (c.d. *Big Data Analysis*), limitando il rischio per la *privacy* degli interessati.

[403] La funzione di *hash* è irreversibile, nel senso che non è possibile risalire dalla stringa di caratteri generati tramite la funzione al contenuto del documento cui la stessa è stata applicata, ma al contempo consente di verificare se un determinato contenuto digitale sia identico a quello alla quale è stata applicata originariamente la funzione. Pertanto, in questo senso, anche l'*hash* è un dato personale.
Cfr., *Working Party* 29, nella propria *Opinion* n. 5/2014 del 10 aprile 2014 ha chiarito che l'*hashing*, così come altre tecnologie, rientra tra le tecniche di pseudonimizzazione (e non di anonimizzazione), in quanto risulterebbero comunque collegabili i dati contenuti nell'*hash* a dati personali esterni allo stesso e, soprattutto, facilmente ricostruibili attraverso un attacco "*brute force*". La soluzione a tale ultimo problema potrebbe essere risolto cifrando i dati prima di attestarli sulla *blockchain* e poi applicando sui dati cifrati la relativa funzione di *hash*. In questo modo il dato diverrebbe inintelligibile e sarebbe messo al sicuro anche contro attacchi "*brute force*", garantendo così l'accesso al dato stesso solo al soggetto titolare della componente privata della chiave di cifratura.
Cfr. SARZANA DI S.IPPOLITO F., NICOTRA M., *Diritto alla blockchain, intelligenza artificiale e IOT*, cit., p. 80.

[404] A questa conclusione perviene anche la Risoluzione del Parlamento UE P8_TA-PROV(2018)0373.

identificabili, anche solo in potenza. Quanto alla tecnica della crittografia (firme digitali, crittografia dei dati, marcatura temporale) essa, invece, consente che un dato crittografato, all'interno della *blockchain*, sia leggibile soltanto da chi possiede la chiave per decifrarlo rappresentando, in questo senso, una misura di sicurezza adeguata a minimizzare il rischio.

Tuttavia, non può sottacersi il fatto che, sebbene indecifrabile, il dato personale criptato continua ad esistere, lasciando aperto la questione sulla sua potenziale decifrabilità una volta distrutta la chiave privata. Diversi Autori, infatti, non hanno esitato a sottolineare che mediante l'aggregazione dei dati di diverso genere, pur "de-identificati" (tra cui i meta-dati dei messaggi crittografati), si può arrivare facilmente "re-identificare" la persona in questione[405].

Indubbiamente il testo del Regolamento europeo sui dati personali costituisce un approccio verso una nuova consapevolezza del valore dei dati nella moderna società tecnologica, in un'ottica di trasparenza e di *accountability* dei soggetti preposti al trattamento[406].

In particolare, il principio di trasparenza è disciplinato degli articoli 12 e segueti del Regolamento, riguardanti il rapporto fra il titolare del trattamento e l'interessato con riferimento all'informazione e all'accesso ai dati[407]. L'operatività di tale principio viene garantita mediante la previsione e la procedimentalizzazione di particolari modalità informative. Invero, il Regolamento prevede che tutte le informazioni destinate al pubblico o al soggetto interessato debbano essere rese facilmente accessibili e comprensibili, espresse mediante un linguaggio semplice e chiaro, soprattutto quando l'informazione degli interessati riguardi l'identità del titolare del trattamento e le finalità dello stesso, nonché le ulteriori informazioni

[405] Cfr., HARDESTY L., *How hard is it to 'de-anonymize' cellphone data?*, in *MIT News*, 27 marzo 2013 in *http://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data*; DE MONTJOYE Y.A. ET AL., *Unique in the Crowd: The privacy bounds of human mobility*, in 3 *Scientific Reports*, 2013, a proposito di uno studio condotto dall'MIT e dell'Università Cattolica di Lovanio (Belgio) le quali procedendo ad un'analisi dei dati sull'utilizzo del cellulare di un milione e mezzo di persone residenti in un piccolo borgo europeo (acquisiti nell'arco di tempo di 15 mesi) è emerso che erano sufficienti per l'identificazione precisa del 95% di loro.

[406] L'art.4 del Regolamento europeo definisce il responsabile del trattamento come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, da solo o insieme ad altri, determina le finalità e i mezzi del trattamento". È inoltre legalmente responsabile del trattamento dei dati.

[407] DI GENIO G., *Trasparenza e accesso ai dati personali*, in Aa.Vv., *La nuova disciplina europea della privacy*, a cura di S. Sica, V. D'Antonio e G.M. Riccio, Milano, 2016, pp. 161 ss.

relative al diritto degli interessati di ottenere conferma e comunicazione del trattamento di dati personali che li riguardano.

In particolare, il Regolamento sottolinea che le persone fisiche debbano essere sensibilizzate rispetto ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Al fine di assicurare che non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati inesatti siano rettificati o cancellati. Essi dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

In particolare, con il termine "liceità" si intende che il trattamento deve essere conforme alla normativa in generale. Sul punto, il Considerando n. 40 afferma che: "perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal presente Regolamento o dal diritto dell'Unione o degli Stati membri, come indicato nel presente Regolamento, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso".

Quando si parla di "correttezza", invece, s'intende che il trattamento deve svolgersi in maniera leale e onesta e la valutazione del rispetto di tale parametro può essere fatta *ex post*, considerando le conseguenze che il trattamento ha avuto sull'interessato. Tale parametro trova anche almeno due punti di riferimento

nell'ambito del nostro ordinamento ed, in particolare, nell'art. 1175 Cod. Civ., a norma del quale "Il debitore e il creditore devono comportarsi secondo le regole della correttezza" e nell'art. 1375 Cod. Civ., ai sensi del quale "Il contratto deve essere eseguito in buona fede"[408].

Infine, richiamando quanto sopra detto, con l'espressione "trasparente" si intende che "le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro".

6. Il principio di *accountability* e la *blockchain*.

Una delle novità principali del GDPR è, senza dubbio, la formalizzazione del principio di *Accountability* o principio di Responsabilizzazione – termine più volte ripetuto in diverse disposizioni del Regolamento –, a norma dell'art. 24.

Dispone, testualmente la norma "Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento".

In sostanza, quindi, il concetto di responsabilizzazione prevede che al titolare del trattamento sia affidato il compito di stabilire, in modo indipendente, le modalità, le garanzie e i limiti del trattamento dei dati e a sua volta gli sia affidato

[408] SOFFIENTINI M., *Privacy: presupposti di legittimità del trattamento dati nella UE*, in *Diritto e Pratica del Lavoro*, 2017, fasc. 38, p. 2265.

il compito di dimostrare di avere adottato misure tecniche ed organizzative adeguate ed efficaci. Sebbene dal testo regolamentare non è facile evincere quale sia la corretta portata dei concetti di adeguatezza ed efficace, in via generale, si può ritenere che le misure adottate dal Titolare possano considerarsi "adeguate" quando tengono conto del contesto e delle circostanze specifiche in cui il trattamento avviene; possono considerarsi "efficaci", quando sono adottare *ex ante* rispetto al trattamento e sono verificate *ex post* rispetto alla loro efficacia[409].

Considerato che non si può avere una piena responsabilizzazione del Titolare se costui non ha proceduto a formalizzare quanto posto in essere, allora il Regolamento ha previsto una serie di disposizioni che richiedono al titolare di raggiungere la *compliance* all'art. 24 attraverso una serie di documentazioni scritte e quindi formali. A titolo esemplificativo, benché non esaustivo, si possono menzionare: 1. l'adozione e quindi la redazione di Codici di condotta – a tal proposito l'art. 24 rinvia all'art. 40 –; 2. la redazione dei Registri del Trattamento, a norma dell'art. 30 del GDPR sia in qualità di Titolare del Trattamento sia, ove sussista, in qualità di Responsabile Esterno; 3. la formalizzazione attraverso apposito atto giuridico dell'eventuale rapporto intercorrente con uno o più Responsabili esterni/interni al trattamento, così come previsto all'art. 28; 4. la formalizzazione di una Valutazione d'impatto sulla protezione dei dati a norma dell'art. 35; 5. attraverso l'elaborazione di specifici modelli organizzativi anche al fine di comprendere quella che potremmo definire come struttura *privacy*, simili a quelli utilizzati nell'applicazione ed elaborazione del Modello Organizzativo previsto dal D.lgs. n. 231 del 2001 ed, infine, anche quanto previsto dall'art. 37 in materia di nomina del Responsabile della protezione dei dati, la quale, come vedremo nel prosieguo della trattazione, altro non è se non una misura stessa di attuazione dell'*accountability*.

Ciò su cui, dunque, il Regolamento pare insistere è che i Titolari devono approcciarsi alla *privacy* in termini non meramente formali, bensì sostanziali, nel

[409] FACCIOLI E., CASSARO M., *Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design*, cit., p. 561.

senso che incombe su di loro il dovere di adottare misure reali e concrete volte a garantire il maggior grado possibile di tutela[410].

Orbene, l'applicabilità del Regolamento alla tecnologia *blockchain* passa attraverso la valutazione del numero degli attori che all'interno della rete possono prendere o meno decisioni. Così nel caso della *blockchain permissioned* (o chiusa) si viene a configurare una contitolarità del trattamento in modo da identificare i ruoli e le responsabilità nel rispetto del GDPR: questa è l'ipotesi sostanzialmente del soggetto (persona fisica o ente) che partecipa ad un consorzio che gestisce una *blockchain* chiusa, o il caso di un consorzio che offre determinati servizi ai suoi utenti finali registrando i dati sulla *blockchain* chiusa.

L'individuazione di ruoli e delle relative responsabilità si rivela, invece, molto più complessa nei casi di *blockchain permissionless* (ad esempio, *Bitcoin*), in quanto, come abbiamo illustrato, queste si connotano per essere "decentralizzate" e aperte: essa, infatti, opera orizzontalmente, non richiedendo la necessità di un organismo di controllo.

Inoltre, dal momento che non può definirsi un *software* ma un protocollo, tale circostanza rimarca ancor di più il mancato carattere di responsabilità dei soggetti nel trattamento dei dati. Gli stessi *miners* (che portano potenza computazionale), gli sviluppatori e gli utenti non possono essere identificati come responsabili del trattamento, in quanto, i primi, si limitano a svolgere un mero ruolo tecnico, mentre di solito gli sviluppatori agiscono sotto pseudonimo e sono muniti di licenza libera. Anche la stessa soluzione di considerare ciascun nodo della *blockchain* come titolare non è parsa idonea ad individuare il soggetto preposto al trattamento.

Il rischio è dunque quello di compromettere anche la possibilità di introdurre la figura del *Data Protection Officer* (DPO) – come del resto impone lo stesso GDPR – deputata ad assistere chi controlla o gestisce i dati al fine di verificare l'osservanza del Regolamento. In particolare, la figura del Responsabile della protezione (RDP, DPO nella versione anglofona) rappresenta una delle novità di maggior spicco del Regolamento. Si tratta di una figura-ufficio, la cui designazione

[410] FACCIOLI E., CASSARO M., *Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design*, cit., p. 561.

diviene obbligatoria nei casi espressamente indicati al paragrafo 1 dell'art. 37: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10[411].

L'art. 37 aggiunge, poi, che, per tutti gli altri casi, non previsti dal testo normativo, "il titolare del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati". Dal punto di vista oggettivo, sono espressamente richieste determinate qualità professionali, in particolare la conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e la capacità di assolvere i propri compiti. Dal punto di vista soggettivo, invece, a norma del paragrafo 6 dell'art. 37 del GDPR, tale figura può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure può essere un soggetto chiamato ad assolvere i compiti individuati sulla base di un contratto di servizi.

I principali compiti e funzioni del RDP consistono: nell'informare e fornire consulenza specialistica al titolare del trattamento o al responsabile nonché ai dipendenti che eseguono il trattamento, sia in merito agli obblighi derivanti dal Regolamento sia, più in generale, nel rispetto dalla normativa nazionale e comunitaria; nella sorveglianza sull'attuazione del Regolamento, sia con riferimento alle misure tecniche – ad esempio riguardo l'adozione del registro dei trattamenti – sia con riguardo alla sensibilizzazione del titolare e del responsabile,

[411] Sul punto cfr. TORTORA A., *Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del "Data Protection Officer" (DPO): incidenza sulla attività della pubblica amministrazione*, Commento a Reg. UE 2016/679, in *Amministrativamente*, 2018, fasc. 5-6, p. 19; BASSINI M., *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni costituzionali*, 2016, fasc. 3, pp. 587 ss.

nonché ai loro dipendenti, in merito agli obblighi regolamentari o provenienti da altre disposizioni in materia di *data protection*. In tal senso, il RPD funge anche da punto di contatto con l'esterno su ogni questione connessa alla materia.

Riconoscendo l'importanza, ma anche la delicatezza, dei compiti che il Responsabile della protezione dei dati è chiamato a svolgere – soprattutto quelli in tema di sorveglianza –, il Regolamento gli riconosce una posizione particolare, così come dispone l'art. 39. In particolare, egli deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni inerenti la materia; deve disporre delle risorse necessarie per assolvere i propri compiti e per accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica; non deve ricevere alcuna istruzione per quanto riguarda l'esecuzione di tali compiti né può essere rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Par tali ragioni, infatti, riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento. Gli interessati possono contattarlo per tutte le questioni inerenti il trattamento dei loro dati personali e all'esercizio dei loro diritti e il RDP è tenuto al segreto o alla riservatezza in merito ai propri adempimenti. Può svolgere altri compiti e funzioni, qualora non diano adito a un conflitto di interessi[412].

Dunque, a ben vedere, il Regolamento crea un ufficio che, non solamente gode di un'adeguata dotazione di risorse umane strumentali per l'espletamento dei suoi incarichi, ma è anche sottratto a qualsiasi indirizzo da parte degli organi di governo e agisce in posizione neutrale nel rispetto delle norme sulla riservatezza[413].

Orbene, per ritornare alle problematiche in esame, a tutte quelle già considerate si aggiungono, altresì, le problematiche di applicazione dei principi individuati dal GDPR, quali la liceità del trattamento secondo un'opportuna base giuridica, gli obblighi in materia di sicurezza, la disciplina del trasferimento dei dati all'estero (essendo la natura di questi *network* quella di assumere dimensioni

[412] Occorre, tuttavia, considerare che il Regolamento non ha introdotto una disciplina di facile comprensione. Invero, di recente, proprio con riferimento alla figura del Responsabile della protezione dei dati (RPD) si è pronunciato il T.A.R. Friuli Venezia Giulia, sentenza n. 287 del 13 settembre 2018, in *www.studiolegale.leggiditalia.it*. In particolare la Corte ha evidenziato che nel Regolamento non sono presenti elementi univoci e condivisi per l'identificazione dei requisiti necessari per una corretta determinazione della figura del RPD.

[413] FIORENTINO L., *Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche*, cit., p. 690.

internazionali), nonché le questioni relativa al diritto di ottenere la rettifica o la cancellazione dei dati inesatti che, come si è detto, mal si concilia con il carattere tecnico di potenziale immutabilità dei dati all'interno delle *blockchain*, con le già evidenziate conseguenze sul diritto all'oblio.

Dunque, le criticità appena rappresentate hanno indotto alcuni operatori del settore a lanciare un appello al legislatore europeo affinché preveda l'esenzione delle tecnologie *blockchain* dal campo di applicazione del Regolamento, anche in ragione del pesante quadro sanzionatorio che esso prevede[414].

[414] Cfr. LIAO S., *Major blockchain group says Europe should exempt Bitcoin from new data privacy rule*, in *https://www.theverge.com*.

CONCLUSIONI

A conclusione del presente lavoro di tesi, si pone la necessità di trarre delle conclusioni, onde ricostruire l'iter seguito nel corso della trattazione e comprendere quale sia lo stato dell'arte della materia qui affrontata.

Come abbiamo visto, intelligenza artificiale e diritto, *smart contracts*, moneta virtuale e *bitcoin*, algoritmi e responsabilità civile rappresentano oggi espressioni di uso pressoché generalizzato e, al tempo stesso, costituiscono oggetto di copiosi studi giuridici. Invero, l'era in cui viviamo, dominata dalla tecnologia, si muove al ritmo del digitale: siamo immersi in una realtà "connessa" attraverso reti ultraveloci e sempre più popolata da programmi ed applicazioni in grado di semplificare operazioni complesse, dematerializzare attività, interagire con l'uomo e, ormai realisticamente, di "apprendere".

Naturalmente anche il diritto è stato prepotentemente coinvolto in questo processo di tecnologizzazione, trovandosi, mai come in questi tempi, ad inseguire una realtà in rapidissima evoluzione, privo per di più di strumenti, finanche lessicali, effettivamente in grado di qualificare e disciplinare fenomeni finora sconosciuti e non riconducibili, se non a patto di forzature che talvolta rischiano persino di apparire inaccettabili, entro schemi tradizionali

L'incessante sviluppo tecnologico cui si è assistito negli ultimi decenni ha fatto sì che si potesse affiancare al tradizionale approccio "morale" al trattamento del dato personale – ossia la concezione che vede nel dato un'esplicazione dell'identità e della personalità del soggetto e, conseguentemente, nel diritto al corretto trattamento dei dati personali un diritto fondamentale – anche l'approccio "negoziale" – che ritiene il dato suscettibile di scambi negoziali aventi rilievo economico e corrispondente a un interesse patrimoniale dei soggetti coinvolti – considerando queste come due facce della stessa medaglia.

La considerazione di questa nuova dimensione non solo consente di svolgere una più coerente analisi giuridico-economica di alcune situazioni, evitando la rapida obsolescenza e recuperando l'effettività di norme che altrimenti non

riuscirebbero a relazionarsi pienamente con le fattispecie concrete, ma consente, altresì, di ampliare il novero delle forme di tutela per l'individuo nel contesto digitale, sempre più, contemporaneamente, utente, consumatore e interessato del trattamento dei dati.

Orbene, come emerso dalla trattazione condotta, per quanto riguarda l'impiego della *blockchain*, uno dei profili di maggiore criticità è costituito dal rispetto della disciplina in materia di *data protection* di cui al Regolamento europeo 2016/679 e alla normativa italiana – ossia il decreto legislativo n. 196 del 2003, cos come modificato dal decreto legislativo n. 101 del 2018 –. A fronte dell'utilizzo della *blockchain* è necessario, infatti, il rispetto dei principi applicabili al trattamento dei dati personali previsti da tale Regolamento, nello specifico dall'art. 5, tra i quali rilevano: la minimizzazione dei dati, secondo cui questi devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, e la limitazione della conservazione, secondo cui i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Alla luce delle esaminate caratteristiche tecnologiche, la *blockchain* pone criticità nel rispetto di tali principi, dal momento che sotto il profilo della minimizzazione dei dati, la difficoltà sta nel fatto che la *blockchain* per il suo funzionamento replica i dati nei vari nodi e, sotto il principio della limitazione della conservazione, i dati, "non alterabili e non modificabili", sono conservati in modo perpetuo. Pertanto, tali aspetti caratteristici della *blockchain*, che costituiscono indubbiamente punti di forza di tale tecnologia, rischiano di trasformarsi in profili di debolezza, capaci di creare complesse problematiche al cospetto dei principi di riferimento della normativa in materia di *data protection*.

Inoltre, in considerazione delle caratteristiche di immodificabilità, inalterabilità e persistenza dei dati nella tecnologia *blockchain*, risultano sostanzialmente inattuabili la rettifica, la limitazione e la cancellazione dei dati stessi e, di conseguenza, il rispetto di tali diritti dell'interessato. In questa tecnologia il procedimento è automatico e proprio tramite automatismi porta alle conseguenze che abbiamo visto.

Anche la vocazione transnazionale della *blockchain*, unita alla pseudonimizzazione, pone problemi, dal momento che è difficile stabilire il luogo del trattamento e la distribuzione dei nodi può allargarsi oltre l'ambito territoriale europeo: emergono difficoltà concrete nell'applicazione della disciplina, che in determinati casi si estende anche fuori dai confini dell'Unione Europea, e dubbi sull'applicazione delle norme afferenti al trasferimento dei dati all'estero del Regolamento 2016/679. D'altro canto, la vocazione transnazionale della *blockchain* porta a ritenere opportuna una regolamentazione sovranazionale, capace di governare in modo effettivo ed efficace un fenomeno che ontologicamente supera i confini territoriali dei singoli Stati, eventualmente integrata da regolazioni nazionali, evitando così un'autoregolazione pericolosa in quanto capace di creare de facto un ordinamento parallelo rispetto a quello giuridico.

Alla luce dell'analisi effettuata nel corso del lavoro, le criticità sul profilo giuridico derivano direttamente dalle caratteristiche tecnologiche che contraddistinguono la *blockchain* e, più in generale, affondano le proprie radici nell'approccio concettuale del Regolamento europeo 2016/679 che prevede un trattamento centralizzato dei dati personali. Va da sé, dunque, che la disciplina in materia di protezione dei dati personali non risulta facilmente adattabile rispetto ad una tecnologia che si caratterizza, invece, proprio per decentralizzazione, disintermediazione e distribuzione.

L'esame delle problematiche che pone il rapporto tra la tecnologia *blockchain* ed il GDPR, impostato su una concezione centralizzata della gestione dei sistemi e piattaforme, fa ritenere certamente non azzardata l'affermazione per cui la norma regolamentare può ritenersi superata dal punto di vista tecnologico ed appare non del tutto adeguata a regolare tali nuovi fenomeni.

D'altra parte anche l'*European Data Protection Supervisor*, nella "*Preliminary Opinion on privacy by design n. 5/2018*" del 31 maggio 2018, ha riconosciuto la *blockchain* come una di quelle tecnologie emergenti, insieme all'intelligenza artificiale ed al *machine learning*, per le quali è necessario uno specifico supporto per lo sviluppo di nuove pratiche e modelli di *business* attraverso la ricerca e l'implementazione di appositi strumenti tecnologici.

E proprio con riferimento alla difficile convivenza tra normativa sulla protezione dei dati personali e *blockchain*, il *report* denominato "*Blockchain Innovation Europe*" del 21 agosto 2018, redatto dall'"*European Union Blockchain Observatory e Forum*" ha espressamente dichiarato che, considerato che in alcuni punti esse appaiono inconciliabili, il compito di trovare un punto di bilanciamento tra le diverse esigenze in gioco non spetta solamente ai giuristi, ma coinvolge anche gli altri attori che si occupano di *Distribuited Ledger Technology*. A tal proposito, il *report* sottolinea, altresì, che la *blockchain* è ancora una tecnologia immatura, e la sua evoluzione potrà senz'altro essere guidata verso il senso di trovare possibili soluzioni in grado di renderla conforme al GDPR.

Ed, in effetti, lungo questa strada si sono mosse proprio alcune tecniche ideate proprio al fine di assicurare una maggiore protezione dei dati personali, in modo da rendere non identificabile il soggetto che effettua la transazione. Si pensi, ad esempio, all'utilizzo di "*one-time accounts*", ossia l'utilizzo di una diversa coppia di chiavi per ciascuna transazione da parte del medesimo soggetto.

La *blockchain* deve, dunque, ritenersi una tecnologia che si pone al di fuori dell'attuale stato dell'arte, posto che sono in atto innumerevoli progetti che prevedono l'aggiunta di funzionalità e caratteristiche assai diverse da quelle attualmente disponibili. Ciò deve indurre l'interprete a considerare pienamente applicabili le eccezioni previste dal GDPR, nei punti in cui richiamano lo stato della tecnica, con l'obiettivo di evitare che interpretazioni troppo rigide della normativa portino ad impedire lo sviluppo dell'innovazione.

Il punto è che nel rapporto tra tecnologia e diritto, se il diritto non deve frenare l'evoluzione, non deve però neppure rinunciare al ruolo che riveste nella società, che si traduce nel riuscire a governare l'evoluzione tecnologica, al fine di tutelare i diritti e prevenire i conflitti, adattandosi senza subirne i mutamenti, al fine di far rispettare i propri principi. In considerazione dell'oggetto da regolare, dovrebbe, pertanto, trattarsi di una regolamentazione atta a contenere i principi giuridici di riferimento, idonei a tutelare i diritti e prevenire i conflitti, rinviando a fonti secondarie e standard la regolazione di dettaglio che necessariamente avrà carattere tecnico.

In considerazione di tutto quanto detto, per superare le criticità esaminate una possibile soluzione è individuabile nell'approccio preventivo, proattivo e tecnico, previsto dallo stesso Regolamento (UE) 2016/679, facendo leva anche in tal caso sull'incorporazione dei principi e delle norme nella tecnologia, in modo che il diritto assolva la funzione preventiva che gli è propria: la regolazione giuridica può servirsi della tecnologia, adattandola al fine di garantire il suo rispetto, in particolare adeguando alcune caratteristiche distintive della *blockchain*, quali disintermediazione e immutabilità, allo scopo di perseguire i principi della *data protection*.

In particolare, dovrebbero essere prospettate soluzioni in grado di conciliare la tecnologia con i principi della protezione dei dati personali, quali la memorizzazione dei dati personali *off-chain*, ossia fuori dalla catena di blocchi, memorizzando sulla stessa un mero riferimento, al fine di garantire l'esercizio dei diritti dell'interessato, oppure tecniche atte a prevenire la re-identificazione dei soggetti che non permettano di ricondurre i dati a un solo soggetto oppure coppie di chiavi diverse per ciascuna transizione.

Più in generale, al fine di consentire l'operatività dei principi del Regolamento europeo andrebbero utilizzate tecniche che permettano di considerare la *blockchain* sufficientemente sicura, tenuto conto di vari parametri obiettivi, quali costi e tempi necessari per riuscire a identificare i soggetti, a seconda delle tecnologie disponibili nel momento storico del trattamento, in modo conforme a quanto previsto dal considerando 26 del Reg. (UE) 2016/679.

D'altro canto, come abbiamo evidenziato nel corso della stesura del lavoro, la *blockchain* favorisce comunque l'integrità e la sicurezza dei dati, la resistenza ad attacchi e il controllo distribuito sugli stessi, in linea con le previsioni in materia di *data protection*. Sotto tale profilo queste tecnologie garantiscono tali aspetti fin dalla progettazione per impostazione predefinita e, di conseguenza, risultano conformi agli obiettivi perseguiti dai principi e dagli strumenti previsti dal Regolamento (UE) 2016/679, come la *data protection by design* e *by default*.

La *blockchain* mostra sicuramente sfide inedite per il diritto, che è necessario affrontare al fine di poter impiegare tale tecnologia e implementare il valore che essa può assumere nella vita quotidiana. È necessario, dunque, mettere

insieme le diverse competenze necessarie (giuridiche ed informatiche) per regolare adeguatamente tali tecnologie emergenti. L'evoluzione tecnologica non è sufficiente se non è accompagnata dallo strumento del diritto, che da sempre, come detto, costituisce il mezzo con cui l'uomo regola la società, al fine di sfruttare in modo strategico e condiviso il potenziale a disposizione, rispettando i diritti e delineando il futuro.

BIBLIOGRAFIA

ABETI R., *L'accesso ai dati personali*, in Cendon (a cura di), *Trattato dei nuovi danni*, II, *Malpractice medica, prerogative della persona, voci emergenti della responsabilità*, Padova, 2011.

ALPA G., *I contratti di utilizzazione del computer*, in *Giurisprudenza italiana*, 1983.

ALPA G., *Sulla qualificazione dei "contratti di informatica"*, in *Economia e diritto terziario*, Roma, 1989.

ALPA G., *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impresa*, 2017.

ALPA G., *Tecnologie e diritto privato*, in *Rivista italiana per le scienze giuridiche*, 2017.

ALPA G., *La "proprietà" dei dati personali,* in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, Milano, 2019.

APARO A., *Il libro delle reti*, Roma, 1995.

ARCELLA G., *GDPR: il registro delle attività di trattamento e le misure di accountability*, in *Notariato*, 2018.

ARCELLA G., MANENTE M., *Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza*, in *Notariato*, 2020.

ARCESE G., *Riflessioni sull'"autonomia" del diritto all'identità personale,* nota a P. Roma, (ord.) 7 gennaio 1984, in *Rassegna di Diritto Civile*, 1985.

ARCUDI G., POLI V., *Il diritto alla riservatezza*, Milano, 2000.

ARENA G., (voce) *Trasparenza amministrativa*, in *Enciclopedia Giuridica Treccani*, vol. XXXI, Roma, 1995.

BALDASSARRE A., *Diritti inviolabili*, in *Enciclopedia giuridica*, XI, Roma, 1989.

BALDASSARRE A., *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974.

BALLARINO T., *Internet nel mondo della legge*, Padova, 2007.

BARGELLI E., *Art. 13 - Diritti dell'interessato*, in Bianca, Busnelli (a cura di), *Tutela della privacy. Commentario alla legge 675/96*, in *Leggi Civili Commentate*, 2019.

BASSINI M., *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni costituzionali*, 2016.

BATTELLI E., D'IPPOLITO G., *Il diritto alla portabilità dei dati personali*, in Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019.

BATTELLI E., INCUTTI E.M., *Gli smart contracts nel diritto bancario tra esigenze di tutela e innovativi profili di applicazione*, in *Contratto e Impresa*, 2019.

BAUMAN Z., *Intervista sull'identità*, Bari-Roma, 2009.

BAVETTA G., *Identità (diritto alla)*, in *Enciclopedia del diritto*, XIX, Milano, 1970.

BECCARA J.L.A., *La privacy nel pubblico. Sintesi dell'integrazione tra codice italiano e regolamento europeo per la pubblica amministrazione*, Milano, 2018.

BELLINI M., *Blockchain & Bitcoin*, Milano, 2018.

BENTIVOGLI M., CHIRIATTI M., *Così la blockchain aumenta l'umanità del lavoro*, in *Il sole 24 ore Commenti del 12 agosto 2018*, *dossier* Manifesto per un nuovo bene pubblico, in *http://www.ilsole24ore.com/art/notizie/2018-08-11/cosi-blockchain-aumenta-l-umanita-lavoro203 658.shtml?uuid=AEBXOWZF*.

BERENTSEN A., SCHAR F., *A Short Introduction to the World of Cryptocurrencies*, in *Federal Reserve Bank of St. Louis Review*, 100(1), 2018.

BERTI SUMAN A., *Indirizzi IP dinamici e cybersicurezza: la conservazione dei "dati personali" degli utenti da parte dell'Internet Provider nel caso Breyer*, in *Orientamenti della Corte di Giustizia dell'Unione Europea in materia di responsabilità civile*, di Alpa G., Conte G., (a cura) Miilano, 2018.

BERTI SUMAN A., *Il diritto alla cancellazione*, in 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.

BIANCA M., *Istituzioni di diritto privato*, Milano, 2014.

BIANCHI L., *Il diritto alla portabilità dei dati*, in 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.

BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto dell'informatica*, 2017.

BOLDRINI N., *Blockchain e GDPR: le sfide e le opportunità per la protezione dei dati*, in *https://www.blockchain4innovation.it/sicurezza/ blockchain -gdpr/*, 2018.

BOMPREZZI C., *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, in *Diritto, mercato e tecnologia*, 2019.

BORRUSO R., *Computer e diritto*, tomo II, Milano, 1988.

BOWER J.L., CHRISTENSEN C.M., *Disrupting Technologies: Catching the Wave*, in *Harvard Business Review*, fasc. I, 1995.

BOWKER G.C., *Data Flakes: An Afterword to "Raw Data" Is an Oxymoron, in Raw data is an oximoron*, a cura di Gitelman, Cambridge-Massachuesetts, 2013.

BOZZOLI J., *La portabilità dei dati personali*, in *Ciberspazio e diritto*, 2019.

BRAVO F., *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2018.

BRAVO F., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018.

BRIGHI R., *Il ruolo dei dati informatici nella costruzione della realtà*, Roma, 2016.

BRYAN M.F., *Island Money*, in *Federal Reserve Bank of Cleveland Research Department*, 2004.

BRUGALETTA F., *Internet per giuristi*, 4a ed., Napoli, 2003.

BUSIA G., *voce Riservatezza (diritto alla)*, in *Digesto delle discipline pubblicistiche*, IV agg., Torino, 2000.

BUTTARELLI G., *Banche dati e tutela della riservatezza*: l*a privacy nella società dell'informazione: commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale*, Milano, 1997.

BUZZACCHI C., *Tecnologia e protezione dei dati personali nella società dei big data. Problemi di profilazione e di garanzia della sicurezza pubblica*, in *Sicurezza e tecnologia*, a cura di Pizzolato, Costa, Milano, 2016.

CAGGIANO I.A., *Il contratto nel mondo digitale*, in *Nuova Giurisprudenza Civile Commentata*, 2018.

CALIFANO L., *Trasparenza e privacy: la faticosa ricerca di un bilanciamento mobile*, in L. Califano, C. Colapietro (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, 2014.

CALIFANO L., *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016.

CALISAI F., *I diritti dell'interessato*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

CALZOLAIO S., *Protezione dei dati personali (diritto pubblico)*, in *Digesto delle discipline pubblicistiche*, Milano, 2017.

CAPAROGNA A., PERAINO L., PERUGI S., CECILI M., ZBOROWSKI G., RUFFO A., *Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione*, in *Diritto Mercato Tecnologia*, 2015.

CARNELUTTI F., *Diritto alla vita privata*, in *Rivista Trimestrale di Diritto Penale*, Milano, 1955.

CARTABIA M., *Le norme sulla privacy come osservatorio sulle tendenze attuali delle fonti del diritto*, in Losano (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001.

CASSANO G., CONTALDO A., *Diritti della persona, internet e responsabilità dei soggetti intermediari*, in *Corriere giuridico*, 2010.

CASTELVECCHI D., *Can we open the black-box of AI?*, in *Nature*, n. 538, 2016, consultabile in *http://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731.*

CASTRONOVO C., *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Europa diritto privato*, 1998.

CATAUDELLA A., *L'uso abusivo di principi*, in *Rivista di diritto civile*, 2014.

CELELLA R., *Il principio di responsabilizzazione: la vera novità del GDPR*, in *Ciberspazio e diritto*, 2018.

CENDON P. (a cura di), *Il quantum nel danno esistenziale*, Milano, 2010.

CERRI A., *Diritto alla riservatezza (diritto costituzionale)*, in *Enciclopedia giuridica*, XXVII, Roma, 1995.

CERRI A., *Riservatezza (diritto alla)*, II, *Diritto comparato e straniero*, in *Enciclopedia giuridica*, XXVII, Roma, 1991.

COLAPIETRO C., *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 22, 2018.

CLACK C.D., BAKSHI V.A., BRAINE L., *Smart Contract Templates: foundations, design landscape and research directions*, in *arXijv.org*, 2016.

CLARIZIA R., *Spunti per uno studio sui contratti di utilizzazione degli elaboratori*, in *Giurisprudenza italiana*, 1983.

CLARIZIA R., *Informatica e conclusione del contratto*, Milano, 1985.

CONTALDO A., CAMPARA F., *Blockchain, criptovalute, smart contract, industria 4.0. Registri digitali, accordi giuridici e nuove tecnologie*, Pisa, 2019.

CORASANITI G., *Il diritto nella società digitale*, Milano, 2018.

CORONA F., *La nuova dimensione della privacy con l'avvento del progresso tecnologico*, Cesena, 2014.

COSTA P., *Diritti fondamentali (storia)*, in *Enciclopedia del diritto*, Annali II, Milano, 2008.

COSTANTINI F.*, Il regolamento (UE) 679/2016 sulla protezione dei dati personali*, in *Lavoro nella Giurisprudenza*, 2018.

COSTANZO P., voce *Internet (diritto pubblico)*, in *Digesto delle discipline pubblicistiche*, Aggiornamento, Torino, 2000.

CRISCI S., *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro Amministrativo*, fasc. 10, 2017.

CRISTOFARI E., *Il diritto alla limitazione del trattamento*, in 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.

CUCCURU P., *Beyond bitcoin: an early overview on smart contracts*, in *International Journal of Law and Information Technology*, 25, 2017.

CUCCURU P., *Blockchain ed automazione contrattuale. Riflessione sugli smart contract*, in *Nuova giurisprudenza civile*, 2017.

CUFFARO V., *Quel che resta di un codice: il d.lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del Codice della Privacy al regolamento sulla protezione dei dati*, in *Corriere Giuridico*, 2018.

D'AMBROSIO M., *Progresso tecnologico, "responsabilizzazione" dell'impresa ed educazione dell'utente*, Milano, 2017.

D'IPPOLITO G., *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Diritto dell'Informazione e dell'Informatica*, fasc. 3, 2020.

D'IPPOLITO G., DI MARTINO G., DOLMETTA M.C., *Evoluzione della disciplina consumeristica e rapporto con la normativa sulla protezione dei dati personali*, in

Consumers' Forum, *Consumerism 2019. Dal codice del consumo al Digital Service Act. Quella dal consumatore al cittadino digitale è vera evoluzione?*, 2019.

DE CUPIS A., *In tema di offesa morale per mezzo della divulgazione cinematografica*, in *Foro italiano*, 1949.

DE CUPIS A., *La verità nel diritto*, in *Foro Italiano*, 1952.

DE CUPIS A., *I diritti della personalità*, Milano, 1982.

DE CUPIS A., *Bilancio di un'esperienza: diritto all'identità personale*, in AA.VV., *La lesione dell'identità personale e il danno non patrimoniale. Atti del seminario promosso dal Centro di iniziativa giuridica P. Calamandrei*, Messina, 16 aprile 1982, Milano, 1985.

DE CUPIS A., *Il diritto all'identità personale,* in SCAGLIARINI S., *La riservatezza e i suoi limiti, sul bilanciamento di un diritto preso troppo sul serio*, Roma, 2013.

DE FILIPPI P., *The interplay between decentralization and privacy: the case of blockchain technologies*, in *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689*, 2016.

DE FILIPPI P., HASSAN S., *Blockchain Technology as a Regulatory Technology. From Code is Law to Law is Code*, 2016, in *http://firstmonday.org/ojs/index.php/fm/article/view/7113*.

DE FILIPPI P., WRIGHT A., *Blockchain and the law*, *The Rule of Code*, Harvard University Press, 2018.

DE FRANCESCHI A., *Il "pagamento" mediante dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

DE GRAZIA L., *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso Internet: argomenti comparativi*, in *Rivista dell'Associazione Italiana dei costituzionalisti*, 2013.

DE MONTJOYE Y.A. ET AL., *Unique in the Crowd: The privacy bounds of human mobility*, in 3 *Scientific Reports*, 2013.

DELL'UTRI M., *Principi generali e condizioni di liceità del trattamento dei dati personali*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

DELFINI F., FINOCCHIARO G., *Diritto dell'informatica*, Milano, 2014.

DI CIOMMO F., *Diritti della personalità tra media tradizionali e avvento di Internet*, in G. Comandé (a cura di), *Persona e tutele giuridiche*, Torino, 2003.

DI CIOMMO F., *Civiltà tecnologica, mercato e insicurezza: la responsabilità del diritto*, in *Rivista Critica di Diritto Privato*, 2010.

DI CIOMMO F., *Quello che il diritto non dice. Internet e oblio*, in *Danno e Responsabilità*, 2014.

DI CIOMMO F., *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

DI CIOMMO F., PARDOLESI R., *Dal diritto all'oblio in Internet alla tutela della identità dinamica. È la rete, bellezza!*, in *Danno e Responsabilità*, 2012.

DI GENIO G., *Trasparenza e accesso ai dati personali*, in Aa.Vv., *La nuova disciplina europea della privacy*, a cura di S. Sica, V. D'Antonio e G.M. Riccio, Milano, 2016.

DI MAJO A., *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in Cuffaro, Ricciuto, Zeno-Zencovich (a cura di), *Trattamento dei dati personali e tutela della persona*, Milano, 1998.

DI PAOLA N., *Blockchain e Supply Chain Management*, Torino, 2018.

DI SABATO D., *Gli smart contracts: robot che gestiscono il rischio contrattuale*, in *Contratto e Impresa*, 2017.

DUHIGG C., *How companies learn your secrets*, The New York Times Magazine, 16 febbraio 2012, consultabile in *http://www.nytimes.com*/.

EENMAA-DIMITRIEVA H., SCHMIDT-KESSEN M.J., *Regulation Through Code as a safeguard for implementing smart contracts in no-trust environments*, in *European University Institute Working Papers*, 2017.

FACCIOLI E., CASSARO M., *Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design*, in *Diritto Industriale*, 2018.

FAINI F., *Blockchain e diritto: la «catena del valore» tra documenti informatici, smart contracts e data protection*, in *Responsabilità Civile e Previdenza*, fasc.1, 2020.

FALCO G., voce *Identità personale*, in *Nuovo Digesto Italiano*, VI, Torino, 1938.

FALZONE E., *Privacy in azienda*, Milano, 2007.

FARO S., *Trattamento dei dati personali e tutela della persona*, in *Digesto delle Discipline Pubblicistiche*, Torino, 2000.

FASSÒ F., *Il regime fiscale dei bitcoins secondo una recente (e unica) prassi amministrativa. Un passo avanti e un'occasione mancata*, in *Strumenti Finanziari e Fiscalità*, 2017.

FAUCEGLIA D., *Il problema dell'integrazione dello smart contract*, in *Contratti*, 2020.

FEROLA L., *Dal diritto all'oblio al diritto alla memoria sul Web. L'esperienza applicativa italiana*, in *Diritto dell'informatica*, 2012.

FERRI G.B., *Diritto all'informazione e diritto all'oblio*, in Rivista di diritto civile, 1990.

FERRI G.B., *Le stagioni del contratto e il pensiero giuridico di G. Alpa*, in *Rivista di diritto commerciale*, 2013.

FICI A., PELLECCHIA E., *Il consenso al trattamento*, in *Diritto alla riservatezza e circolazione dei dati personali*, I, Milano, 2003.

FINOCCHIARO G., *I contratti ad oggetto informatico*, Padova, 1993.

FINOCCHIARO G., *I contratti informatici*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia*, diretto da F. Galgano, vol. XXII, Padova, 1997.

FINOCCHIARO G., *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su Internet*, in *Contratto e Impresa in Europa*, 2001.

FINOCCHIARO G., *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Diritto dell'Informatica*, 2012.

FINOCCHIARO G., *Diritto all'anonimato. Anonimato, nome, identità personale*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia*, Galgano (diretto da), Padova, 2008.

FINOCCHIARO G., *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012.

FINOCCHIARO G., *Riflessioni su diritto e tecnica*, in *Diritto informatico e dell'informatica*, 2012.

FINOCCHIARO G., *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove Leggi Civili Commentate*, 2017.

FINOCCHIARO G., *Il contratto nell'era dell'intelligenza artificiale*, in *Rivista Trimestrale di Diritto e Procedura Civile*, fasc.2, 2018.

FINOCCHIARO G., *Intelligenza artificiale e diritto - Intelligenza artificiale e protezione dei dati personali*, in *Giurisprudenza Italiana*, 2019.

FINOCCHIARO G., *Riflessioni sugli smart contract e sull'intelligenza artificiale*, in *Giustiziacivile.com*, 16 novembre 2020.

FINCK M., *Blockchains and Data Protection in the European Union*, *Max Planck Institute for Innovation & Competition Research Paper* No. 18-01, in *European Data Protection Law Review*, 1/2018.

FIORE C., *Riservatezza (diritto alla)*, in *Enciclopedia giuridica*, Agg., XXVII, Roma, 1998.

FIORENTINO L., *Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche*, in *Giornale di diritto amministrativo*, 2018.

FLORIDI L., *The 4th Revolution. How infosphere is reshaping human reality*, Oxford, 2014.

FOIS S., CHIOLA C., ESPOSITO C., *Sulla libertà di manifestazione del pensiero,* in SCAGLIARINI S., *La riservatezza e i suoi limiti, sul bilanciamento di un diritto preso troppo sul serio*, Roma, 2013.

FONDERICO G., *La regolazione amministrativa del trattamento dei dati personali*, in *Giornale di Diritto Amministrativo*, 2018.

FRAIOLI M., *Il diritto di opposizione e la revoca del consenso*, in *Cittadinanza europea*, 2018.

FRANCO P., *Understanding Bitcoin. Cryptoghraphy, Enginnering and Economics*, Padstow, 2014.

FRANCESCHELLI V. (a cura di), *La tutela della privacy informatica*, Milano, 1988.

FROSINI V., *Informatica diritto e società*; Milano, 1988.

FROSINI V., *Banche dati e tutela della persona*, in *Informatica, diritto e società*, Milano, 1992.

FROSINI V., *Note critiche al disegno di legge sulla protezione dei dati personali*, in *Diritto dell'informatica*, 1992.

FUERGIUELE L., *I contratti a conclusione telematica*, in F. Bocchini, *Diritto dei consumatori e nuove tecnologie*, I, *Gli scambi*, Torino, 2002.

FURFARO S., *voce Riservatezza*, in *Digesto discipline penalistiche*, Agg. II, Torino, 2008.

FUSARO A., *Nome e identità personale degli enti collettivi. Dal "diritto" all'identità uti singuli al "diritto" all'identità uti universi*, in *Nuova Giurisprudenza Commentata*, 2002.

GABRIELLI E., RUFFOLO U., *Intelligenza Artificiale e diritto*, in *Giurisprudenza Italiana*, Luglio 2019.

GALGANO F., *La cultura giuridica italiana di fronte ai problemi informatici (considerazioni di sintesi)*, in AA. VV., *I contratti di informatica. Profili civilistici, tributari e di bilancio*, a cura di Alpa G. e Zeno-Zencovich V., Milano, 1987.

GALIMBERTI U., *Psiche e techne: l'uomo nell'età della tecnica*, Milano, 1999.

GAMBINO A., *L'accordo telematico*, Milano, 1997.

GAMBINO A.M., BOMPREZZI C., *Blockchain e protezione dei dati personali*, in *Diritto informatico e dell'informatica*, 2019.

GAMBINI M., *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *Espaço Jurídico*, 2013.

GARAVAGLIA R., *Tutto su blockchain*, Milano, 2018.

GAROFALO L., *GDPR, e se la Blockchain non fosse conforme al regolamento?*, in *key4biz.it/gdpr-e-se-la-blockchain-non-fosse-conforme-al-regolamento /222368/*, 2018.

GAROFALO D., *Blockchain, smart contract e machine learning: alla prova del diritto del lavoro*, in *Lavoro nella Giurisprudenza*, 2019.

GASPARRI G., *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, in *Il diritto dell'informazione e dell'informatica*, 2015.

GEORGE D., REUTIMANN K., TAMÒ-LARRIEUX A., *GDPR bypass by design? Transient processing of data under the GDPR*, in *International Data Privacy Law*, 2019.

GIACOBBE G., *L'identità personale tra dottrina e giurisprudenza. Diritto sostanziale e strumenti di tutela*, in AA.VV., *La lesione dell'identità personale e il danno non patrimoniale. Atti del seminario promosso dal Centro di iniziativa giuridica P. Calamandrei*, Messina, 16 aprile 1982, Milano, 1985.

GIANNANTONIO E., *Il progetto di legge sulle banche di dati personali e le normative straniere*, in *Giurisprudenza italiana*, 1985.

GIANNONE CODIGLIONE G., *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in *Diritto dell'Informazione e dell'Informatica*, fasc. 4-5, 2015.

GIOVANNANGELI S.F., *L'informativa agli interessati e il consenso al trattamento*, in 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.

GIOVANNELLA F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, *I dati personali nel diritto europeo*, Milano, 2019.

GIULIANO M., *La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio*, in *Diritto informatico e dell'informatica*, 2018.

GRECO G.L., *Monete complementari e valute virtuali*, in *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, a cura di Paracampo, Torino, 2017.

GROSSO E., *Autorità indipendente o autorità onnipotente? Il potere normativo di fatto del Garante per la protezione dei dati personali*, in Losano (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001.

GUZZO A., *Il Documento Programmatico sulla Sicurezza*, in *Lo Stato civile italiano*, 2010.

HANCE O., *Internet e la legge*, Milano, 1996.

HARARI Y.N., *21 lezioni per il XXI secolo*, Milano, 2018.

HOFFMAN R., *Why the blockchain matters*, in *Wired*, 15 febbraio 2015.

IBÁÑEZ, KIERON O'HARA L.D., SIMPERL E., *On Blockchains and the General Data Protection Regulation*, in *https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf*, 2018.

IRTI N., *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, 2006.

KARABOGA M.,MATZNER T., OBERSTELLER H., OCHS C., *Is There a Right to Offline Alternatives in a Digital World?*, in *Data Protection and Privacy: (In)visibilities and Infrastructures*, a cura di Leenes, van Brakel, Gutwirth, De Hert, Springer, 2017.

HARDESTY L., *How hard is it to 'de-anonymize' cellphone data?*, in *MIT News*, 27 marzo 2013 in *http://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data.*

KELLY K., *New Rules for the New Economy: 10 Radical Strategies for a Connected World*, Penguin Books, 2004.

KEYNES J.M., *Treatise On Money*, Vol. II, 1930.

KOCHERLAKOTA N., *The Technological Role of Fiat Money*, in *Federal Reserve Bank of Minneapolis, Quarterly Review* 22:3, 1998.

LEMME G., *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Rivista di diritto bancario*, 2016.

LESSIG L., *Code and Other Law of Cyberspace*, New York, 1999.

LIAO S., *Major blockchain group says Europe should exempt Bitcoin from new data privacy rule*, in *https://www.theverge.com*.

LIBRANDO V., *La tutela della riservatezza nello sviluppo tecnologico*, in *Diritto dell'informatica*, 1987.

LIPARI N., *Le categorie del diritto civile*, Milano, 2013.

LO SURDO C., *Gli strumenti di tutela del soggetto "interessato" nella legge e nella sua concreta applicazione*, in Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, I, Milano, 2003.

LO SURDO C., *Gli strumenti di tutela del soggetto "interessato" nella legge e nella sua concreta applicazione*, in Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, 2018.

LOSANO M.G., *I progetti di legge italiani sulla riservatezza dei dati personali*, in Alpa, Bessone (a cura di), *Banche dati, telematica e diritti della persona*, Padova, 1984.

LOSANO M.G., *Il diritto privato dell'informatica*, Torino, 1986.

LOSANO G., *Un progetto di legge sulla protezione dei dati personali*, in *Diritto dell'informatica*, 1987.

LOSANO M.G., *Introduzione*, in Giannantonio, Losano, Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla l. 675/1996*, Padova, 1997.

LUCCHINI GUASTALLA E., *Privacy e data protection: principi generali*, in Tosi (a cura di), *Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019.

MANCINI N., *Bitcoin: rischi e difficoltà normative*, in *Banca impresa società*, 2016.

MANENTE M., *L. 12/2019 - Smart Contract e tecnologie basate su registri distribuiti. Prime note, Studio 1_2019*, in *Consiglio Nazionale del Notariato*, 2019.

MANTELERO A., *GDPR tra novità e discontinuità - Gli autori del trattamento dati: titolare e responsabile*, in *Giurisprudenza Italiana*, 2019.

MARCHETTI G., *Diritto di cronaca on-line e tutela del diritto all'oblio*, in AA.VV., in *Da Internet ai social network*, Sant'Arcangelo di Romagna, 2013.

MARTINELLI S., *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in internet e le problematiche poste dalla de-indicizzazione*, in *Diritto dell'informatica*, 2017.

MARTINOTTI G., *La difesa della privacy*, in *Politica del Diritto*, 1972.

MASTROPAOLO E., *Identità personale e manifestazione del pensiero. Strumenti di tutela*, in *Diritto Informatico e dell'Informatica*, 1985.

MASTRORILLI D., *Contrattazione a distanza. Disciplina consumeristica e di settore*, Bari, 2011.

MATTIUZZO F., VERONA N., *Blockchain e smart contract: nuove prospettive per il rapporto di lavoro*, in *Lavoro nella Giurisprudenza*, 2019.

MAXWELL W., SALMON J., *A guide to blockchain and data protection*, in *https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf*, 2018.

MAZZAMUTO S., *Il principio del consenso e il problema della revoca*, in *Libera circolazione e protezione dei dati personali*, I, Milano, 2006.

MCAFEE A., BRYNJOLFSSON E., *Big data: the management revolution*, in *Harvard Business Review*, n. 10, 2012.

MESSINETTI D., *Oggetto dei diritti*, in *Enciclopedia del diritto*, XXIX, Milano, 1979.

MESSINETTI D., *Personalità (diritti della)*, in *Enciclopedia del diritto*, XXXIII, Milano, 1983.

MESSINETTI R., *Circolazione dei dati personali e autonomia privata*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, Milano, 2019.

MEIJER D.B., *Consequences of the implementation of the Blockchain technology. Mater Thesis*, Delft University of Technology, 2017.

MEZZANOTTE M., *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009.

MILLARD C., *Blockchain and law: incompatible codes?*, in *Computer Law & Security Review*, 34, 2018.

MIRABELLI G., *Contratto tra terminali e documento elettronico*, in *Rivista notariato*, 1986, p. 120, di AA.VV., a cura di G. Alpa, V. Zeno-Zencovich, *I contratti di informatica: profili civilistici, tributari e di bilancio*, Milano, 1987.

MIRABELLI G., *In tema di tutela dei dati personali note a margine della proposta modificata di direttiva CEE*, in *Diritto dell'informatica*, 1993.

MIRABELLI G., *Le posizioni soggettive nell'elaborazione elettronica dei dati*, in *Diritto dell'informatica*, 1993.

MODUGNO F., *I "nuovi diritti" nella giurisprudenza costituzionale*, Torino, 1995.

MONEA A., *Regolamento n. 2016/679: la necessità di uno specifico "modello organizzativo" per la protezione dei dati personali*, in *Azienditalia*, 2018.

MONTALCINI C., SACCHETTO F., *Bitcoin e criptovalute*, in *Diritto tributario telematico*, a cura di Montalcini e Sacchetto, Torino, 2017.

MONTANARO D., *Il diritto di accesso ai dati personali e il diritto di rettifica*, in 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.

MONTELEONE A.G., *Il diritto alla portabilità dei dati. Tra diritti della personalità e diritti del mercato*, in *Luiss law review*, 2017.

MONTUORI L., SIANO M., *Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione*, in G. Busia, L. Liguori, O. Pollicino, *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, 2016.

MORELLI M.R., *Oblio (diritto all')*, in *Enciclopedia del Diritto*, Agg. VI, Milano, 2002.

MORELLI A., *I diritti e la Rete. Notazioni sulla bozza di Dichiarazione dei diritti in Internet*, in *Federalismi.it*, fasc. 1, 2015.

MORMILE L., *I diritti dell'interessato*, in Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, 2006.

MORO VISCONTI R., *La valutazione delle blockchain: internet of value, network digitali e smart transaction*, in *Diritto Industriale*, 2019.

MOSCON V., *Tecnologie blockchain e gestione digitale del diritto d'autore e connessi*, in *Diritto Industriale*, 2020.

NASTRI M., *Identità personale, identità digitale e identificazione elettronica alla luce del decreto semplificazioni*, in *Notariato*, 2020.

NERVI A., *I diritti dell'interessato*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *Il Codice del trattamento dei dati personali*, Torino, 2007.

NEWELL S., MARABELLI M., *Strategic opportunities (and challenges) of algorithmic decision-making: a call for action on the long-term societal effects of "datification"*, in *Journal of Strategic Information Systems*, 24/2015.

NICOTRA M., *Blockchain e GDPR: le norme da conoscere per tutti i problemi*, in *https://www.agendadigitale.eu/sicurezza/blockchain-e-gdpr-le-norme-da-conoscere-per-tutti-i-problemi/*, 2018.

NOWIŃSKI W., KOZMA M., *How Can Blockchain Technology Disrupt Existing Business Models?*, in *Entrepreneurial Business and Economics Review*, 5(3), 2017.

NUCCI G., *GDPR: struttura e contenuti del d.lgs. n. 101/2018*, in *Azienditalia*, 2018.

O'KEEFE C.M., *Privacy and Confidentiality in Service Science and Big Data Analytics*, in J. Camenisch, S. Fischer-Hubner, M. Hansen, *Privacy and Identity Management for the Future Internet in the Age of Globalization*, London, 2015.

PACE A., *Art. 15*, in G. Branca (a cura di), *Commentario della Costituzione italiana*, Roma-Bologna, 1977.

PAGANO R., *Tutela dei dati personali: evoluzione della legislazione europea e stato del dibattito in Italia*, in *Informatica e diritto*, Milano, 1986.

PALLADINO A., *L'equilibrio perduto della blockchain tra platform revolution e GDPR compliance*, in *Rivista di diritto dei media*, 2019.

PARDOLESI R., *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003.

PAROLA L., MERATI P., GAVOTTI G., *Blockchain e smart contract: questioni giuridiche aperte*, in *Contratti*, 2018.

PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità,* in Pardolesi R., *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003.

PARDOLESI R., MOTTI C., *L'informazione come bene*, in G. De Nova (a cura di), *Dalle res alla new properties*, Milano, 1991.

PASCUZZI G., *Il diritto dell'era digitale*, Bologna, 2002.

PASQUINO T., *Identità digitale della persona, diritto all'immagine e reputazione*, in Tosi (a cura di), *Privacy digitale*, Milano, 2019.

PELLECCHIA E., *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove Leggi Civili Commentate*, 2020.

PERLINGIERI G., *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015.

PEZZOLI E., *Internet of Things, tecnologia blockchain e diritti IP*, in *Diritto Industriale*, 2020.

PIATTI L., *Blockchain, decentralizzazione e privacy: un nuovo approccio del diritto*, in *Ciberspazio e diritto*, vol. 19, n. 60, 2018.

PICA G., voce *Internet (diritto penale)*, in *Digesto delle discipline penalistiche*, Milano, 2004.

PICARO R., *I contratti ad oggetto informatico*, in F. Bocchini, *Diritto dei consumatori e nuove tecnologie*, I, *Gli scambi*, Torino, 2002.

PINO G., *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003.

PINO G., *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in *Libera circolazione e protezione dei dati personali*, I, Milano, 2006.

PINO G., *L'identità personale*, in *Trattato di biodiritto*, diretto da Rodotà S., Zatti P., *Ambito e fonti del biodiritto*, a cura di Rodotà, Tallacchini, Milano, 2010.

PIRAINO F., *La liceità e la correttezza*, in Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, 2006.

PIRAINO F., *Per una teoria della ragionevolezza in diritto civile*, in *Europa e Diritto Privato*, 2014.

PIRAINO F., *Buona fede, ragionevolezza e "efficacia immediata" dei principî*, Napoli, 2017.

PIRAINO F., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuova Giurisprudenza Commentata*, 2017.

PIRAINO F., *GDPR tra novità e discontinuità - I "diritti dell'interessato" nel Regolamento Generale sulla Protezione dei dati personali*, in *Giurisprudenza Italiana*, 2019.

PIRODDI P., *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, in *Diritto dell'Informatica*, 2015.

PISA M., JUDEN M., *Blockchain and Economic Development: Hype vs. Reality*, in *Center for Global Development Policy Paper*, 2017.

PIZZETTI F. (a cura di), *Il caso del diritto all'oblio*, Torino, 2013.

PIZZETTI F., *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

PROSPERI M., *Il dibattito italiano sull'esistenza e sul fondamento del diritto alla riservatezza prima del suo espresso riconoscimento*, in *www.privacy.it.*

RAVÀ A., *Istituzioni di diritto privato*, Padova, 1938.

RAZZINI A., *Blockchain e protezione dei Dati personali alla luce del nuovo regolamento europeo GDPR*, in *Ciberspazio e diritto*, vol. 19, n. 60, 2018.

RESTA G., *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Rivista Critica di Diritto Privato*, 2000.

RESTA G., *Autonomia privata e diritti della personalità*, Napoli, 2005.

RESTA G., *Identità personale e identità digitale*, in *Il Diritto dell'Informazione e dell'Informatica*, 2007.

RESTA G., *Dignità, persone, mercati*, Torino, 2014.

RESTA G., ALPA G., *Le persone fisiche e i diritti della personalità*, Milano, 2019.

RESTA G., ZENO-ZENCOVICH V. (a cura di), I*l diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015.

RESTA G., ZENO-ZENCOVICH V., *Volontà e consenso nella fruizione dei servizi in rete*, *in Rivista trimestrale di diritto e procedura civile*, fasc. 2, 2018.

RICCI A., *I diritti dell'interessato*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, opera diretta da Finocchiaro, Bologna, 2017.

RICCIO G.M., PEZZA F., *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*, in Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019.

RICCIUTO V., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Diritto dell'Informazione e dell'Informatica*, fasc. 4, 2018.

RINALDI G., *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contratto e Impresa*, 2019.

RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica di diritto privato*, 1997.

RODOTÀ S., *Tecnopolitica, la democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004.

RODOTÀ S., *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy*, in *Europa e Diritto Privato*, 2004.

RODOTÀ S., *Intervista su privacy e libertà*, a cura di Conti, Roma-Bari, 2005.

RODOTÀ S., *Il diritto di avere diritti*, Roma-Bari, 2012.

RODOTÀ S., *Il mondo della rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014.

RODOTÀ S., *Quattro paradigmi per l'identità*, in *Vivere la democrazia*, Bari, 2018.

RODOTÀ S., *Controllo e privacy della vita quotidiana. Dalla tutela della vita privata alla protezione dei dati personali*, in *Rivista Critica di Diritto Privato*, 2019.

ROOSENDALE A., *Digital personae and profiles as representations of individuals*, in *Privacy and identity management for life*, 2010.

ROPPO E., *Diritti della personalità, diritto all'identità personale e sistema dell'informazione. Quale modello di politica del diritto?*, in Alpa, Bessone, Boneschi, Caiazza (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983.

ROVEGNO A.O., *Identità digitale: tra esigenze di condivisione e necessità di tutela*, in *Cyberspazio e Diritto*, 2013.

RUBINO DE RITIS M.R., *Virtuale, la quarta generazione di moneta*, in *Rivista del Notariato*, fasc. 6, 2018.

RUBINO DE RITIS, *La moneta digitale complementare: modelli convenzionali di adempimento in criptomonete e prospettive per il sud*, in Aa.Vv., Fintech a cura di Fimmanò e Falcone, Napoli, 2019.

RUSSO B., *L'evoluzione dei sistemi e dei servizi di pagamento nell'era digitale*, Padova, 2020.

RUSSO P., *I danni esistenziali*, Torino, 2014.

SALITO G., voce *Smart Contracts*, in *Digesto italiano, discipline privatistiche, sezione civile*, Torino, 2019.

SALZANO G., *I diritti dell'interessato*, in Monducci, Sartor (a cura di), *Il codice in materia di protezione dei dati personali. Commentario sistematico al D.Lgs. 30 giugno 2003 n. 196*, Padova, 2004.

SAMMARCO P., *Privacy digitale, motori di ricerca e social network: dal diritto di accesso e rettifica al diritto all'oblio condizionato*, in Tosi (a cura di), *Privacy*

digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy, Milano, 2019.

SARTOR G., *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, II ed., Torino, 2010.

SARZANA F., *La Blockchain*, in Ippolito S., Nicotra M., *Diritto della Blockchain, intelligenza artificiale e IoT*, Milano, 2018.

SASSANO F., *Il diritto all'oblio tra internet e mass media*, Vicalvi 2015.

SAVORANI G., *I contratti dell'informatica*, in *I contratti in generale*, a cura di G. Alpa, M. Bessone, Agg. 1991-1998, vol. II, Torino, 1999.

SCAGLIARINI S., *La riservatezza e i suoi limiti, sul bilanciamento di un diritto preso troppo sul serio*, Roma, 2013.

SENIGAGLIA R., *Il Reg. UE 2016/679 e il diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Leggi Civili Commentate*, 2017.

SESSO SARTI O., *Profilazione e trattamento dei dati personali*, in L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017.

SGUERSO F., *Il contratto telematico. Le moderne tecnologie e il "vecchio" codice civile*, in *www.aicsweb.it/documenti/2012.*

SIMBULA M., *Dati personali: pull vs. push*,, in *https://studiolegalesimbula.com /dati-personali-pull-vs-push*/, 2017.

SIMONATI A., *L'accesso amministrativo e la tutela della riservatezza*, Trento, 2002.

SIMONCINI A., *Autorità indipendenti e costruzione dell'ordinamento giuridico: il caso del Garante per la protezione dei dati personali*, in *Diritto Pubblico*, fasc. 3, 1999.

SIROTTI GAUDENZI A., *Proprietà intellettuale e diritto della concorrenza*, Padova, 2010.

SOFFIENTINI M., *Privacy*, Milano, 2016.

SOFFIENTINI M., *Privacy: presupposti di legittimità del trattamento dati nella UE*, in *Diritto e Pratica del Lavoro*, 2017.

STAZI A., *Automazione contrattuale e "contratti intelligenti". Gli smart contract nel diritto comparato*, Torino, 2019.

STAZI A., CORRADO F., *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Diritto dell'Informazione e dell'Informatica*, fasc. 2, 2019.

STEINER C., *Automate this. How algorithms came to rule our world*, Penguin, 2012.

SUNGWOOD K., *Game Theory Solutions for the Internet of Things: Emerging Research and Opportunities*, Hershey, 2017.

SZABO N., *Smart Contracts: Building Blocks for digital markets*, in *http://www.fon.hum.uva.nl/rob/Courses/ InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html*, 1996.

TAPSCOTT D., TAPSCOTT A., *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, 2016, Portfolio.

THIENE A., *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, Ferrara, 2017.

THOBANI S., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Genova, 2018.

TORINO R., *Il diritto di opposizione al trattamento dei dati personali e il diritto a non essere sottoposti a decisioni basate su trattamenti automatizzati e alla profilazione nel Regolamento (UE) 2016/679*, in *Cittadinanza europea*, 2018.

TORTORA A., *Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del "Data Protection Officer" (DPO): incidenza sulla attività della pubblica amministrazione*, Commento a Reg. UE 2016/679, in *Amministrativamente*, 2018.

TOSI E., *I contratti di informatica*, Milano, 1993.

TOSI E., *Il contratto virtuale* (parte 1), in *Studium Juris*, 2008.

TOSI E., *Contratti informatici, telematici e virtuali*, Milano, 2010.

TRAVERSI A., *Il diritto dell'informatica*, Milano, 1985.

TRIPODI E.M., *Formulario dei contratti d'informatica e del commercio elettronico*, 3° ed., Roma, 2002.

WALPORT M., *Distributed ledger technology: Beyond blockchain*, in *UK Government Office for Science*, 2016.

WARREN S., BRANDEIS L.D., *«The Right to Privacy»*, *Harvard Law Review*, fasc. 4, 1890.

WERBACH K., CORNELL N., *Contracts Ex Machina*, in *Duke Law Journal*, 2017, p. 67, consultabile su *https://papers.ssrn.com*

WITTEN I. H., FRANK E., HALL M., PAL C., *Data Mining. Practical Machine Learning Tools and Techniques* 4, Morgan Kaufmann-Elsevier, 2017.

VAN LIESHOUT M., *The Value of Personal Data,* in J. Camenisch, S. Fischer-Hubner, M. Hansen, *Privacy and Identity Management for the Future Internet in the Age of Globalization*, London, 2015.

VARDI N., *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin*, in *Il diritto dell'informazione e dell'informatica*, 2015.

VEALE M., BINNS R., AUSLOOS J., *When data protection by design and data subjects rights clash*, in *International Data Privacy Law*, 2018.

VECCHI P., *Art. 1- Finalità e definizioni*, in Bianca, Busnelli (a cura di), *Tutela della privacy. Commentario alla legge 31 dicembre 1996, n. 675*, in *Leggi Civili Commentate*, 1999.

VENIER O., *Intelligenza artificiale, blockchain e mondo IoT: l'esperienza degli operatori*, in *Diritto Industriale*, 2020.

VETTORI G., *Privacy e diritti dell'interessato*, in *Responsabilità Civile e Previdenza*, 1998.

VIGEVANI G.E., *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano*, in *Danno e Responsabilità*, 2014.

VIOLA F., *Data mining. Sottrazione, cessione e utilizzo di dati*, in *Diritto alla riservatezza e progresso tecnologico*, a cura di Fumagalli Meraviglia, Napoli, 2015.

ZATTI P., *Dimensioni ed aspetti dell'identità nel diritto privato attuale*, in *Nuova Giurisprudenza Commentata*, 2007.

ZENO ZENCOVICH V., *Sul rilievo pratico o sistematico della categoria dei c.d. contratti di informatica*, in AA.VV., *I contratti di informatica. Profili civilistici, tributari e di bilancio*, a cura di Alpa G. e Zeno-Zencovich V., Milano, 1987.

ZENO-ZENCOVICH V., *Profili negoziali degli attributi della personalità*, in *Diritto dell'Informazione e dell'Informatica*, 1993.

ZENO-ZENCOVICH V., *voce Informazione (profili civilistici)*, in *Digesto delle discipline privatistiche*, sezione civile, IX, Torino, 1993.

ZENO ZENCOVICH V., «*Identità personale*», in *Digesto delle discipline civilistiche*, IX, Torino, 1995.

ZYSKIND G., NATHAN O., PENTLAND A.S., *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, in *https://ieeexplore.ieee.org/document/7163223*/, 2015.

INDICE GIURISPRUDENZIALE

T.A.R. Friuli Venezia Giulia (sentenza n. 287 del 13 settembre 2018, in *www.studiolegale.leggiditalia.it.*

TAR Lazio, sezione I, sentenza del 10 gennaio 2020 n. 261, in *Quotidiano Giuridico*, 2020