rivista di diritto alimentare
www.rivistadirittoalimentare.it
Anno XIII, numero 1 · Gennaio-Marzo 2019
25

Gli utilizzi della Blockchain e dell'Internet of Things nel settore degli alimenti

Giuseppe Spoto

1.- Blockchain e nuove tecnologie

Il presente lavoro si propone di analizzare le possibili applicazioni delle nuove tecnologie nel settore alimentare, con una particolare attenzione alle implicazioni della blockchain e delle nuove potenzialità offerte dall'Internet of Things. Il giurista è chiamato oggi al compito di valutare l'impatto che le nuove tecnologie sono destinate a produrre, adattando le categorie giuridiche tradizionali o fornendo interpretazioni in grado di dare risposte esaurienti di fronte ad problemi inediti.
L'obiettivo principale che ha animato inizialmente gli ideatori di Bitcoin[1] è stato rivolto alla realizzazione di un sistema di transazioni[2] in grado di funzionare tra gli operatori senza intermediazioni bancarie, attraverso uno scambio *one to one*, fondato sulla reciproca fiducia e sulla certezza del risultato finale. La blockchain[3] è nata per raggiungere questo scopo, ma successivamente sono stati valorizzati anche ulteriori utilizzi, perché questa tecnologia consente di realizzare un registro immodificabile, organizzato in nodi separati che formano una catena che può essere adoperata in un'ampia gamma di ambiti[4].
Più semplicemente, possiamo dire che la blockchain è costituita da una rete di computer, che approvano una transazione in un registro pubblico, consultabile da tutti i nodi della rete. Ogni volta che un computer si aggiunge alla rete, scarica un esemplare del registro e diventa un nodo, con la possibilità di verificare e certificare le transazioni. Ciascun nodo può accedere alle registrazioni condivise nella catena e possedere una copia identica, anche se in realtà, il meccanismo è più complesso di ciò che si è qui descritto, e sarebbe più opportuno distinguere tra diverse forme di validazione delle transazioni, mediante blockchain[5]. Infatti, dovremmo distinguere la tec-

(1) Cfr. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org.pdf mentre per gli aspetti giuridici connessi all'utilizzo di Bitcoin e Blockchain si rinvia a: S. Capaccioli, *Criptovalute e bitcoin. Un'analisi giuridica*, Milano, Giuffré, 2015; N. Busto, *Bitcoin tra disintermediazione e iper-intermediazione*, in *Cyberspazio e Diritto*, Vol. 17, n. 56, 2016, 309 ss. Una blockchain è un registro (ledger) costituito da diversi nodi (block) collegati in maniera sequenziale e immutabile tra di loro e che realizza una catena (chained), contenente informazioni digitali di qualsiasi tipo.
(2) Il consenso delle transazioni all'interno della blockchain può avvenire mediante il meccanismo *proof-of-work*, in cui i vari nodi sono in competizione e che consente di modificare la catena, aggiungendo un ulteriore blocco quando un nodo riesce a comunicare per primo la soluzione di un algoritmo matematico e il modello *proof-of-stake*, che consente di modificare la catena, aggiungendo un blocco mediante la validazione delle transazioni, ma soltanto a beneficio di alcuni nodi. La blockchain, attraverso un sistema di codificazione e crittografia, permette così di registrare e certificare l'esistenza di una determinata informazione. Tutte le transazioni, per essere effettuate, devono essere condivise in rete ed accettate. Una volta validate, le transazioni sono immodificabili perché per modificare fraudolentemente le informazioni dovrebbero essere modificati contemporaneamente i nodi della rete. Rispetto ad altre simili tecnologie, la blockchain è un sistema grandemente decentralizzato, che può essere transnazionale e che è al contempo in grado di funzionare senza l'intervento di terzi intermediari, legando i partecipanti, tramite un sistema *peer-to-peer*, in cui ciascun soggetto che costituisce un nodo della catena può creare e validare le transazioni, custodire e tenere memoria di tutte le relative informazioni.
(3) Non esiste ancora una disciplina europea chiara in merito, anche se la Commissione europea ha costituito il "EU Blockchain Observatory and Forum" per studiare meglio il fenomeno ed è stata approvata la Risoluzione del Parlamento europeo sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione - 2017/2772(RSP).
(4) Per un approfondimento sul funzionamento della "blockchain": H. Diedrich, *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*, Wildifire Publishing, 2016.
(5) Ai fini di una corretta classificazione è importante distinguere, a seconda della tipologia di tecnologia utilizzata, perché la blockchain pubblica è un network aperto, in grado di certificare le informazioni che possono essere conosciute da tutti liberamente, mentre nella blockchain privata, soltanto alcuni interessati possono accedere e consultare le informazioni. Per una disamina dei vantaggi e degli svantaggi tra le diverse tipologie cfr. F. Sarzana di S. Ippolito – M. Nicotra, *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018, 22 ss.

rivista di diritto alimentare
www.rivistadirittoalimentare.it
Anno XIII, numero 1 · Gennaio-Marzo 2019

nologia "permissionless" in cui tutti i partecipanti possono validare le transazioni, dalla tecnologia "permissioned", in cui soltanto alcuni soggetti possono validare le transazioni, ed in cui la partecipazione al network è chiusa. Da ultimo, esiste anche una tecnologia che utilizza un modello ibrido tra i primi due, in cui alcuni nodi hanno un'influenza maggiore rispetto ad altri. Tale sistema può essere accessibile al pubblico o rimanere a beneficio solamente dei partecipanti.
Il meccanismo della blockchain presuppone che tutti i partecipanti attivi abbiano un esemplare del registro e che le informazioni non possano essere copiate o modificate apertamente. Le modifiche potranno avvenire solo in modo coordinato e qualora si dovesse verificare un tentativo di accedere da parte di un soggetto non abilitato ovvero l'inserimento in un nodo di informazioni illegittime, tale intervento verrebbe riconosciuto immediatamente dagli altri nodi della rete, in quanto le informazioni introdotte sarebbero difformi da tutte le altre copie del registro. Un'informazione inserita nella Blockchain potrebbe essere manomessa soltanto modificando la metà più uno di tutti i nodi che compongono la catena, ma per far ciò occorrerebbe una potenza di calcolo elevatissima di un unico soggetto. L'utilizzo delle tecnologie crittografiche consente quindi la piena tracciabilità dei dati e la sicurezza delle informazioni inserite[6].
Tra i principali vantaggi della blockchain[7] vi è la particolare versatilità e la possibilità di utilizzare questo strumento anche per certificare i diversi passaggi dei prodotti lungo le filiere. In particolare, la blockchain consente di realizzare obiettivi di decentralizzazione, trasparenza, sicurezza e immutabilità dei dati.

2.- I molteplici utilizzi della blockchain

Dal punto di vista degli utilizzi in ambito alimentare[8], la blockchain potrebbe trovare applicazione in numerosi campi, come ad esempio: l'approvvigionamento, i processi di produzione, il controllo della qualità degli alimenti e delle fasi del trasporto, la gestione dei resi e il riutilizzo dei rifiuti[9].
L'applicazione del protocollo HACCP[10] (*Hazard analysis and critical control points*) è uno dei

([6]) In base all'articolo 41 del regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica.
([7]) D. Tapscott – A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is changing Money, Business, and the World*, 2016, 30 s. considerano vantaggi della *blockchain*: la fiducia che questa tecnologia è in grado di assicurare; il decentramento dei poteri che non si concentrano nelle mani di un unico soggetto, attraverso un meccanismo *peer to peer*; la possibilità di ottenere incentivi partecipando al *network*; la garanzia della privacy coniugata con la trasparenza attraverso pseudonimi; la possibilità di implementare *smart contract*; una maggiore diffusione della ricchezza e la realizzazione di un capitalismo ben distribuito.
([8]) Va segnalato che gli esempi sono numerosi. Ricordiamo a questo proposito che Carrefour ha sviluppato un progetto di ricerca che prevede l'utilizzo della blockchain per controllare le informazioni relative alla filiera di un particolare tipo di pollo, dotando le relative etichette di un codice leggibile dai consumatori con lo smartphone e che negli Stati Uniti, Walmart ha utilizzato la blockchain per la vendita di prodotti freschi.
([9]) La Legge 19 agosto 2016, n. 166, Disposizioni concernenti la donazione e la distribuzione di prodotti alimentari e farmaceutici a fini di solidarietà sociale e per la limitazione degli sprechi, è stata introdotta in Italia per agevolare la cessione gratuita delle eccedenze alimentari in modo da contrastare il dispendio dei prodotti non acquistati e favorire un loro riutilizzo. Per un approfondimento del tema si rinvia a: L. Costantino, *La problematica degli sprechi nella filiera agroalimentare. Profili introduttivi*, Bari, 2018; A. Di Lauro, *Lo spreco alimentare: il ruolo della "norma" sulle determinanti personali e sociali dei comportamenti alimentari,* Atti del convegno, XV World Congress of Agricultural Law, Umau, Poznan, 2018, 432; P. Lattanzi, *Gli ostacoli di ordine giuridico alla riduzione dello spreco alimentare*, in *Riv. dir.agr.*, 2014, 273 s.; G. Maccioni, *La lotta allo spreco alimentare tra strategie di regolazione e governance*, in *Riv. dir. agrario*, 2017, 633; Id., *Spreco alimentare. Regole e limiti nella transizione verso modelli agroalimentari sostenibili*, Torino, 2018; F. Pepe, *Approvata la legge contro lo spreco alimentare*, in *q. Riv.* www.rivistadirittoalimentare.it, n. 3-2016, 56 s.; G. Strambi, *Limiti e regole nella distribuzione delle eccedenze alimentari*, in *Nutridialogo*, *Il Diritto incontra le altre scienze su Agricoltura, Alimentazione ed Ambiente*, a cura di A. Di Lauro, Pisa, 2016, 35 s.
([10]) La Direttiva 93/43/CEE del Consiglio, del 14 giugno 1993, sull'igiene dei prodotti alimentari ha introdotto i principi del controllo dei "punti critici", sottolineando l'importanza di una analisi dei passaggi fondamentali della filiera produttiva ed esaltando i vantaggi dell'autocontrollo e dell'auto-organizzazione delle imprese.

rivista di diritto alimentare
www.rivistadirittoalimentare.it
Anno XIII, numero 1 · Gennaio-Marzo 2019

sistemi maggiormente utilizzati per garantire la sicurezza in ambito alimentare, così da presentare al consumatore un prodotto che sia stato realizzato e controllato nel rispetto di standard determinati. Anche in questo settore, la blockchain potrebbe rendere il sistema più efficiente, fornendo una piattaforma di supporto in grado di tracciare i passaggi nella preparazione degli alimenti.
Infatti, il sistema delle informazioni registrate attraverso una catena di nodi potrebbe spingere verso l'unificazione dei controlli e la realizzazione di un registro unitario più efficiente.
L'utilizzo della Blockchain potrebbe contribuire a realizzare gli obiettivi di introduzione di un unico sistema integrato dei controlli, individuato dal Regolamento n. 2017/625, che come è noto è stato approvato soprattutto per semplificare e razionalizzare i controlli di fronte alla eccessiva pluralità delle fonti, dopo l'introduzione del Pacchetto igiene e delle successive integrazioni[11].
In altre parole, la blockchain consentirebbe di attuare, in modo sistemico, un'effettiva integrazione degli strumenti di controllo ufficiali del settore agro-alimentare, non soltanto a fini igienico-sanitari, ma anche in tema di qualità dei prodotti[12]. In questo modo diminuirebbe il ruolo fondamentale di supervisione e coordinamento esterno, perché anche in assenza di tali accertamenti, potrebbero essere parimenti garantiti controlli elevati e imparziali.
Sotto il profilo della trasposizione dei principi alla prassi, il risultato porterebbe a garantire un sistema pienamente conforme agli obiettivi del Regolamento Ue n. 625 del 2017 che, oltre a prevedere l'istituzione di soggetti con compiti di vigilanza frontaliera, promuove l'adozione di sistemi informatici unificati per il trattamento delle informazioni e forme più ampie di collaborazione tra Stati membri, comprese attività di formazione congiunta.
La tecnologia Blockchain potrebbe essere anche utilizzata per contrastare i fenomeni della contraffazione, dell'adulterazione e della sofisticazione dei prodotti, garantendo la certificazione della corretta conservazione durante il trasporto delle merci, la registrazione dei prodotti da commercializzare, e un monitoraggio lungo l'intera *supply chain*, fornendo un utile aiuto per contrastare i pericoli di possibili manipolazioni.
Sappiamo che in ambito alimentare, vi sono alcuni prodotti che devono mantenere nel trasporto una determinata temperatura e la *supply chain* potrebbe essere sviluppata in modo da controllare l'esatto rilevamento della temperatura durante lo spostamento, evidenziando gli eventuali punti deboli. Un altro modo per rendere il trasporto dei prodotti più celere ed efficace, attraverso le nuove tecnologie, consisterebbe nel sostituire la documentazione di accompagnamento della merce in forma cartacea con la digitalizzazione dei documenti. L'utilizzo della blockchain garantirebbe così l'integrità delle informazioni documentali[13].
Si potrebbero identificare rapidamente lotti specifici in qualsiasi fase, rintracciare eventuali prodotti scaduti o contaminati, eliminandoli dalla distribuzione. La realizzazione di libri mastri pubblici decentralizzati nel settore alimentare spingerebbe così in generale ad innalzare gli standard qualitativi, rendendo i consumi più accessibili e sicuri.
Fin dal Libro Bianco sulla sicurezza alimentare[14], la Commissione ha richiamato la necessità di una

([11]) In punto v. M. Gioia, *Prime note sul regolamento n. 625/2017*, www.rivistadga.it, 4/2017; F. Albisinni, *Il Regolamento (UE) 2017/625: controlli ufficiali, ciclo della vita, impresa e globalizzazione*, in *q. Riv.* www.rivistadirittoalimentare.it, n. 1-2018, pag. 11.
([12]) I. Canfora, *Gruppi di produttori ed enti di certificazione: competenze e legittimazione in una regolazione mobile*, in *q. Riv.* www.rivistadirittoalimentare.it, n. 2-2015, pag. 4.
([13]) Tra le piattaforme che hanno sperimentato maggiormente i benefici delle nuove tecnologie si può certamente ricordare NewCo5, nata nel 2013, con l'obiettivo di sviluppare e migliorare la tracciabilità di alcuni prodotti e di certificarne la qualità. La piattaforma utilizza il modello di blockchain pubblica per monitorare i passaggi dei prodotti identificati mediante l'attribuzione di un'identità digitale. Le informazioni che i consumatori possono reperire riguardano l'impresa produttrice, il prodotto e il processo di produzione, nonché tutti i passaggi della filiera, fino ad arrivare al consumatore finale. Tra le applicazioni più celebri sviluppate da NewCo5 va annoverato il monitoraggio del pesce fresco, mediante un sistema che si attiva quando i pescatori inviano attraverso cellulare l'informazione sul tipo di pesce catturato e sul momento della pesca. A partire da questa prima comunicazione, il pesce viene "seguito" lungo tutti i passaggi della supply chain, dalla pesca fino al consumo finale.
([14]) Libro bianco sulla sicurezza alimentare [COM (1999) 719 definitivo].

rivista di diritto alimentare
www.rivistadirittoalimentare.it
Anno XIII, numero 1 · Gennaio-Marzo 2019

politica alimentare efficace, guardando alla rintracciabilità dei percorsi dei mangimi e degli alimenti, nonché dei loro ingredienti, come un aspetto fondamentale e imprescindibile, ma nonostante l'individuazione di questi obiettivi, le difficoltà per una piena rintracciabilità di tutti gli ingredienti degli alimenti composti sono rimaste molteplici.

Il sistema di rintracciabilità degli ingredienti, malgrado l'evoluzione degli interventi normativi e l'approvazione di regole generali in tema di etichettatura, continua ad essere differenziato in relazione ai vari prodotti, con costi destinati a ricadere sui prezzi al consumo, in modo ancora eccessivamente sproporzionato rispetto ai benefici auspicati dalla disciplina introdotta[15].

Un utilizzo delle nuove tecnologie permetterebbe non soltanto di verificare che il prodotto acquistato sia sicuro per il consumatore, ma anche che il trasporto sia avvenuto regolarmente, riuscendo a risalire dettagliatamente all'origine degli ingredienti, come ad esempio al tipo specifico di farina utilizzata per realizzare una determinata confezione di biscotti.

Un sistema di rintracciabilità piena, in direzione della massima trasparenza, con ridotte criticità, potrebbe essere realizzato, ricorrendo alla blockchain e alla combinazione di algoritmi appropriati. Rimarrebbero comunque da risolvere alcuni problemi, ad esempio in merito alla compatibilità rispetto alle norme UNI che si applicano a tutti i settori industriali, commerciali e del terziario, ma non al settore elettrotecnico ed elettronico di competenza del CEI. Pure su questo punto, considerando che la blockchain è una tecnologia che utilizza la connessione tra personal computer, sarebbe necessario un aggiornamento, in modo da chiarire quali disposizioni seguire, evitando sovrapposizioni tra norme che sono nate per disciplinare ambiti diversi.

L'osservazione non è banale e dimostra le difficoltà che il diritto incontra di fronte ad una realtà in continuo cambiamento, dove le risorse tecnologiche crescono ad una velocità straordinaria, ponendo l'interprete davanti ad inediti problemi da risolvere.

In futuro potrebbero sorgere consorzi per la creazione di blockchain private, condivise soltanto tra partecipanti interni. In queste ipotesi, la trasparenza e la gestione delle informazioni riguarderebbero soltanto le relazioni tra questi ultimi, a meno che non venga garantita la possibilità di comunicazione con altri consorzi sviluppatori di ulteriori blockchain. È evidente che le possibilità di applicazione di questi meccanismi in base agli obiettivi perseguiti sono molteplici.

La Blockchain potrà facilitare gli interventi delle Autorità garanti di valutazione della legittimità degli atti dei consorzi di tutela dei prodotti tipici. Come è noto, esistono a livello nazionale numerosi organismi associativi che vedono la partecipazione di imprenditori agricoli[16]. In questa categoria rientrano anche i consorzi tra i produttori[17] che svolgono funzioni di promozione, monitoraggio e controllo dei prodotti tutelati. La Blockchain può essere in grado di potenziare e rendere più efficienti non soltanto i controlli interni tra i partecipanti al consorzio, ma anche il monitoraggio esterno dell'AGCM[18], facilitando l'avvio di eventuali istruttorie dirette ad applicare la disciplina

([15]) Sul punto si rinvia in particolare a quanto osservato da: L. Costato, *La rintracciabilità degli alimenti*, in *Trattato di Diritto agrario*, III, Torino, 2011, pp. 539, 540, secondo cui l'organizzazione dei grandi produttori di alimenti non può essere certamente accostata alle difficoltà dei piccoli laboratori, costretti a sostenere costi in proporzione maggiori per adattarsi al regime previsto.

([16]) Le informazioni trasferite mediante connessioni tra computer potrebbero essere utilizzate, ad esempio, anche nell'ambito delle c.d. "certificazioni di gruppo" dell'agricoltura biologica, rafforzando il rapporto fiduciario tra produttori e consumatori. Sul tema delle certificazioni di gruppo si rinvia a: L. Petrelli, "*La certificazione di gruppo: una nuova opportunità per i piccoli produttori biologici europei?*", in *q. Riv.* www.rivistadirittoalimentare.it, n. 2-2015, pag. 50.

([17]) L. Paoloni, *Consorzi fra produttori agricoli*, in *Digesto civ.*, Agg., I, Torino, 2000, 215; Id., *I consorzi fra produttori agricoli tra passato e presente*, in AA.VV., *Agricoltura e diritto*, Scritti in onore di Emilio Romagnoli, II, Milano, 2000, 895 ss.

([18]) Per un approfondimento di questi aspetti si veda: L. Costantino, *Il ruolo dell'Autorità Garante della Concorrenza e del Mercato nel settore agroalimentare*, in "Trattato di Diritto agrario", diretto da L. Costato – A. Germanò – E. Rook Basile, Torino, 2011, 236; G. Sepe, *Il controllo del potere di mercato nella filiera agro-alimentare: profili concorrenziali e ruolo dell'AGCM*, in in *q. Riv.* www.rivistadirittoalimentare.it, n. 1-2013, pag. 35.

della concorrenza[19] anche ai consorzi di tutela della qualità, nel quadro delle regole della concorrenza tra le imprese, per evitare intese restrittive ed assicurando imparzialità e terzietà.
La violazione delle regole a tutela della concorrenza o la mancata osservanza delle norme del disciplinare potrebbero essere monitorate in modo capillare, consentendo controlli anche per quantitativi ridotti, mettendo in atto un sistema di effettiva trasparenza e consentendo prontamente di sanzionare ed intervenire di fronte ad eventuali anomalie.

3.- Criticità di un sistema complesso che può essere ancora migliorato.

Nonostante la blockchain offra numerosi vantaggi, contribuendo alla circolazione di prodotti alimentari sicuri e tutelando consumatori e produttori, esistono ancora numerosi ostacoli che si frappongono per l'utilizzo e lo sviluppo di tale tecnologia.
Alcuni problemi sono in generale connessi al fatto che il sistema non è ancoro diffuso in modo generalizzato e maturo, pertanto, in termini di gestione ed implementazione[20] occorre un più maturo rodaggio. Questi limiti connessi alla fase iniziale di attuazione sono ovviamente destinati con il tempo ad essere neutralizzati, ma vi sono altri problemi di carattere tecnico che sono certamente più difficili da superare, soprattutto se pensiamo alla realizzazione di catene di nodi troppo grandi. Infatti, anche se è vero che tutti i nodi registrano le stesse informazioni mediante duplicazioni istantanee, occorre costatare che il registro delle transazioni "si accresce" con i successivi passaggi. Un eccessivo numero di transazioni potrebbe determinare un immagazzinamento abnorme di dati e un appesantimento della catena con il rischio di un rallentamento del sistema di validazione. La crescita della capacità degli hard disk, infatti, è avvenuta costantemente nel tempo, ma in modo indirettamente proporzionale allo sviluppo della blockchain.
È indubbio che questo modello di decentramento permetta di realizzare transazioni sicure senza intermediari, ma è anche vero che la totale assenza di un soggetto esterno con l'incarico di vigilare sulla corretta esecuzione delle regole, potrebbe presentare alcuni punti di debolezza in fase operativa, soprattutto nell'ipotesi in cui avvenga un qualsiasi imprevisto del meccanismo automatico di cooperazione dei computer-nodi.
Se è vero che lo sviluppo di una blockchain aperta è in grado di assicurare la creazione di un network orizzontale, in cui tutti i computer-nodi presentano gli stessi poteri senza possibilità di supremazia e abuso da parte di nessuno, quando invece si realizzano meccanismi di tipo *permissioned* si formano catene in cui soltanto alcuni partecipanti hanno la possibilità di validare le transazioni, con il rischio di non assicurare a tutti i soggetti membri i medesimi poteri, vanificando proprio gli aspetti maggiormente vantaggiosi della nuova tecnologia.
Di contro, più aperta (e quindi potenzialmente più grande) è la catena e maggiori saranno gli ostacoli per un corretto monitoraggio, a causa dell'elevato numero dei soggetti coinvolti, soprattutto se i nodi operano in aree geografiche lontane, applicando, per quanto riguarda la specifica realtà imprenditoriale, regole nazionali diverse. Se invece si parla di una *supply chain* non troppo grande, che assicuri la possibilità di registrare ogni singolo passaggio di un prodotto, in maniera immodificabile, permettendo di conoscere che cosa è stato esattamente trasferito da un operatore ad un altro, in quale momento e a quale prezzo, è evidente che la tecnologia blockchain è molto vantaggiosa, perché può consentire a tutti i protagonisti della "catena", indipendentemente dalla funzione e dal ruolo svolto (produttori, trasportatori, fornitori e perfino consumatori finali) di

([19]) I. Canfora, *La disciplina della concorrenza nel Diritto comunitario*, in *Trattato di Diritto agrario*, diretto da L. Costato - A. Germanò - E. Rook Basile, Torino, 2011, 209 s.
([20]) Per una valutazione dei limiti della Blockchain cfr. N. Di Paola, *Blockchain e supply chain management*, Milano, 2018, 80 s.

rivista di diritto alimentare
www.rivistadirittoalimentare.it
Anno XIII, numero 1 · Gennaio-Marzo 2019

reperire le informazioni inerenti le transazioni avvenute, in modo trasparente ed efficace. Questo utilizzo permetterebbe di garantire la piena tracciabilità dei prodotti[21] senza ostacoli. Ulteriori vantaggi potrebbero essere assicurati, integrando la blockchain con alcuni strumenti suppletivi, come ad esempio i c.d. "smart contracts"[22], che consentirebbero correttivi in via automatica, in grado di alleggerire e contrastare eventuali rallentamenti, senza però far venir meno la garanzia di sicurezza. Introdurre ad esempio un algoritmo di automatismo in tema di pagamento alla consegna della merce potrebbe assicurare tempi di realizzazione delle operazioni più fluidi[23].

Esiste anche il rovescio della medaglia in un sistema basato su contratti fondati esclusivamente su algoritmi[24]: il rischio di generare strumenti privi del tutto dei requisiti della discrezionalità dei contraenti, e tale caratteristica potrebbe produrre problemi ben più gravi in termini di effettiva libertà negoziale. Vi sono quindi ancora numerose criticità per quanto riguarda gli aspetti giuridici connessi allo sviluppo di queste tecnologie. Ad esempio, sotto il profilo delle regole della concorrenza, una *blockchain permissioned* potrebbe consentire la formazione di cartelli tra operatori, impedendo la partecipazione di eventuali concorrenti attraverso l'inibizione dell'accesso alla piattaforma. Di contro, l'eccessiva decentralizzazione e frammentazione di una *blockchain permissionless* garantirebbe i medesimi poteri a tutti i partecipanti, compresi i soggetti che non hanno investito sufficienti risorse per implementare la rete, che sfrutterebbero i benefici derivanti dal lavoro altrui[25].

([21]) In realtà, sotto il profilo tecnico, sarebbe più corretto parlare di tracciabilità di filiera. Per il concetto di "tracciabilità di prodotto" si rinvia al Regolamento n. 820/97 e al Regolamento n. 1760/2000. A partire dal Regolamento n. 178/2002 è stato precisato un ulteriore regime di tracciabilità che distingue la nozione di tracciabilità di prodotto applicabile alla carne bovina, dalla nozione di tracciabilità di filiera applicabile alla generalità dei prodotti alimentari. Cfr. F. Albisinni, *Strumentario di diritto alimentare europeo*, Milano, 2017, 181 s. Una ulteriore specificazione è adoperata per distinguere il termine "tracciabilità", utilizzato per indicare il percorso che va dalla materia prima al prodotto finale, dal termine "rintracciabilità", per indicare il percorso a ritroso dall'alimento finito alla materia prima. È fuori dubbio che lo sviluppo della tecnologia blockchain e l'ampia gamma di possibili applicazioni alla catena alimentare potrebbero determinare in futuro una modifica della nomenclatura finora utilizzata in direzione di una maggiore precisione.

([22]) Nick Szabo ha utilizzato per primo l'espressione "smart contract" per classificare i contratti definiti "intelligenti", in cui le transazioni vengono eseguite automaticamente. Cfr. S. Capaccioli, *Smart contracts: traiettoria di un'utopia divenuta attuabile*, in *Cyberspazio e Diritto*, Vol. 17, n. 55, 2016, 25 ss.; L. Piatti, *Dal codice Civile al codice binario: blockchain e smart contracts*, in *Cyberspazio e Diritto,* Vol. 17, n. 56, 2016, 325 ss.

([23])Il Parlamento europeo, con la Risoluzione del 16 febbraio 2017, ha fornito una serie di raccomandazioni per l'applicazione dei principi della robotica e degli algoritmi in ambito giuridico. Si definisce *smart contract* un contratto governato da algoritmi che permettono di combinare una serie di variabili nell'interesse dei contraenti. Per quanto riguarda le fonti di diritto interno si veda il Decreto-Legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla L. 11 febbraio 2019, n. 12, che all'art. 8 ter definisce "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili. Nel successivo comma è definito: "*smart contract*" un programma per elaboratore 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. Gli *smart contract* soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale.

([24]) Non sono mancate le voci critiche, se pensiamo a: D. De Kerckhove, A. Kroker, E. Morozov, D. Gambetta, T. Maldonado che, con argomentazioni differenti, contestano la natura agnostica dell'algoritmo e il modello della decisione robotica estesa ad ogni ambito della conoscenza umana, ritenendo che queste nuove tecnologie potrebbero spingere verso una vera e propria "*datacrazia*". Per quanto riguarda gli orientamenti giurisprudenziali più recenti, per il Consiglio di Stato, sez. VI, sentenza 8 aprile 2019, n. 2270 una decisione amministrativa può essere assunta mediante l'utilizzo di un algoritmo, purché conoscibile. La regola algoritmica è assoggettata al pieno sindacato del giudice amministrativo. Per quanto riguarda l'utilizzo di algoritmi in processi decisionali del settore pubblico si veda la sentenza del 22 marzo 2017 n. 3769 del TAR, Lazio-Roma, sez. III bis, che ha stabilito che il Ministero è tenuto a rendere noto l'algoritmo con cui viene gestita la mobilità dei docenti, nonché la riflessione del Consiglio di Stato nelle sentenze n. 9224, 9225, 9226, 9227, 9228, 9229 del 10 settembre 2018 che ha contestato l'utilizzo di un impersonale algoritmo per lo svolgimento dell'intera procedura di assegnazione dei docenti alle sedi disponibili nell'organico dell'autonomia della scuola.

([25]) Va in realtà precisato che gli effetti negativi dipendono sempre dal modo in cui la tecnologia è utilizzata. Pertanto, fermo restando le osservazioni svolte, in tema di tutela del diritto d'autore, brevetti e opere dell'ingegno, la blockchain potrebbe offrire numerosi vantaggi, garantendo la capacità di collegare un prodotto al suo autore, mediante un *hash* registrato dalla catena dei nodi.

rivista di diritto alimentare
www.rivistadirittoalimentare.it
Anno XIII, numero 1 · Gennaio-Marzo 2019

4.- Responsabilità, certificazioni e controlli

La Blockchain permette di validare le informazioni sia sotto il profilo temporale, sia sotto il piano della immodificabilità dei dati, ma non garantisce la correttezza e la veridicità delle informazioni e quindi non è uno strumento utilizzabile in senso proprio ai fini della certificazione. Se estendiamo il discorso fin qui svolto alle nuove tecnologie in generale e alla loro eventuale combinazione, diventa indispensabile interrogarsi sulle modalità di connessione tra le differenti teconologie, valutando di conseguenza l'impatto che esse sono destinate ad avere in materia di certezza del diritto.
In via preliminare possiamo ricordare che il sistema delle certificazioni nel settore agroalimentare è garantito attraverso specifici organismi di controllo[26] e applica regole primariamente di diritto pubblico. In Italia, gli organismi di controllo sono autorizzati ad operare dal Ministero delle politiche agricole e forestali, e in attuazione del Regolamento europeo 765/2008[27], il sistema di accreditamento si avvale di un ente unico denominato Accredia, a cui è stato affidato, sotto la vigilanza del Ministero dello sviluppo economico, il ruolo di attestare la competenza e l'imparzialità degli organismi di certificazione, di ispezione e di verifica, nonché dei laboratori di prova e taratura.
L'utilizzo delle nuove tecnologie nell'ambito del diritto alimentare, se da un lato potrà ridurre la distanza tra il modello della tracciabilità del prodotto e quello della tracciabilità di filiera, dall'altro versante è destinato a generare nuovi problemi in merito alle fonti e al controllo delle basi di dati informatizzate. Le applicazioni della Blockchain per il settore agroalimentare possono riguardare sia le filiere verticalmente integrate, sia le filiere regolamentate. Tuttavia, rimangono numerosi problemi concreti sul modello di Blockchain da adottare per quanto riguarda la validazione delle informazioni (permissionless o permissioned), e per quanto riguarda i rapporti tra partecipanti (modello centralizzato o distribuito). Dalla scelta del modello, mediante l'accesso a tutti o soltanto ad alcuni partecipanti della filiera, dipenderà ovviamente l'effettivo grado di trasparenza realizzato.
Lo sviluppo delle nuove tecnologie informatiche di sistemi volontari di tenuta dei dati finirà per facilitare la possibilità di estendere alla tracciabilità di filiera gli aspetti propri del modello di tracciabilità di prodotto, smussando le differenze tra i modelli esistenti, ma comporterà un evidente stravolgimento delle regole finora promosse, perché il compito di tenuta di tali basi di dati informatizzate può essere eseguito da soggetti meramente privati.
L'implementazione delle nuove tecnologie determinerà rilevanti ricadute in riferimento a tutte le varie forme di tracciabilità[28] (esterna ed interna all'azienda), non soltanto a partire dalle informazioni inerenti l'immissione delle merci nel mercato, ma anche alla possibilità di monitorare il percorso seguito dagli ingredienti per arrivare a costituire il prodotto finale.
Fino ad oggi, come già detto, si è trattato prevalentemente di passaggi gestiti (direttamente) dal settore pubblico ovvero affidati (indirettamente) a soggetti terzi delegati, come gli organismi di certificazione e fermo restando, le ipotesi di autocontrollo[29] vi è stato un maggior *favor* per le "certezze" promananti dall'attività delle autorità pubbli-

([26]) Per un approfondimento della regolazione in materia di accreditamento degli organismi di certificazione si rinvia alle relazioni pubblicate in *q. Riv.* www.rivistadirittoalimentare.it, n. 4-2011 e n.1-2012 del convegno del dicembre 2011, presso l'Università della Tuscia, sul tema: "Controlli, certificazioni, responsabilità: tra pubblico e privato, tra domestico e globale".
([27]) S. Amorosino, "*Il regolamento CE n.765/2008,in materia di accreditamento degli organismi di "valutazione della conformita`"* (certificazione), in *q. Riv.* www.rivistadirittoalimentare.it, n. 4-2011, p. 24.
([28]) Il quadro disciplinare dei controlli, relativi alla tracciabilità del prodotto e alla tracciabilità di filiera, ha finora riguardato principalmente la responsabilità delle imprese, generando costi per queste ultime. Per quanto riguarda i costi sostenuti dai produttori, per le certificazioni affidate ad organismi privati o pubblici, sono stati avanzati dalla dottrina i medesimi rilievi critici mossi per il sistema delle società di rating. Sul punto si veda L. Ammannati, *Mercati finanziari, società di rating, autorità ed organismi di certificazione*, in *q. Riv.* www.rivistadirittoalimentare.it, n. 1-2012, 31.
([29]) Va precisato che il c.d. "autocontrollo" e il sistema HACCP (Hazard analysis and critical control points) non sono termini equivalenti, perché "autocontrollo" ha un'accezione più ampia ed è un concetto obbligatorio per tutti gli operatori coinvolti nella filiera della produzione alimentare, mentre l'HACCP ha un'accezione più ristretta e vale solo per gli Operatori dei settori post-primari.

che[30], piuttosto che per quelle derivanti da fonti di carattere privato, ma è evidente che in futuro, proprio su questo fronte, dovranno essere svolte riflessioni suppletive. Così, dall'evoluzione normativa e dalla sovrapposizione di regole di matrice differente, si è andata affermando la coesistenza di ambiti disciplinari al contempo privatistici e pubblicistici[31].

Il quadro composto è caratterizzato dall'emersione di nuovi centri regolatori e di nuovi meccanismi di verifica, e pone problemi in merito ai profili di responsabilità sia del soggetto privato gestore della piattaforma informatica contenente dati di rilievo pubblico, sia dei soggetti che possono direttamente inserire dati nel sistema. L'utilizzo di un modello decentrato formato da una catena di nodi attraverso la costituzione di una blockchain, in cui non sia materialmente possibile identificare un gestore unitario sovraordinato rispetto ai singoli partecipanti, non può risolvere di certo i dubbi sulla responsabilità del controllo della piattaforma, anzi paradossalmente proprio tale meccanismo rischia di amplificare il problema, mediante il coinvolgimento di tutti i nodi nella circolazione delle informazioni, ma nei confronti dei quali non è "tecnicamente" possibile attribuire responsabilità individuali di gestione dei dati. A tale preoccupazione, è strettamente collegata la questione della pluralità dei soggetti capaci di immettere dati nel sistema.

Anche nell'ipotesi in cui sia individuato un soggetto "formalmente" responsabile della "certificazione" di dati che circolano a mezzo di canali telematici e informatici, rimane da capire se possa essere applicato il regime introdotto dal Codice dell'Amministrazione Digitale (CAD), oppure sia sufficiente richiamare le norme generali in tema di responsabilità civile[32].

L'art. 30 del decreto legislativo 7 marzo 2005, n. 82[33] (CAD) considera responsabile per il danno cagionato a chi abbia fatto ragionevole affidamento, il certificatore che rilascia al pubblico un certificato qualificato o che comunque garantisce al pubblico l'affidabilità del certificato. Tale norma introduce una specifica disciplina in tema di responsabilità del certificatore, stabilendo che quest'ultimo risponde dell'inadempimento in caso di danno concreto, se non prova di avere agito senza colpa o dolo. L'onere della prova della mancanza di dolo o colpa incombe quindi sull'autore del danno e non sul danneggiato in base ai principi del Codice dell'amministratore digitale.

Si può però facilmente replicare che le disposizioni del Codice dell'amministrazione digitale sono nate per disciplinare uno specifico ambito di rapporti con la Pubblica Amministrazione, e non certo per essere estese alle certificazioni dei soggetti privati, pertanto sarebbe improprio ampliare il loro ambito di applicazione al di fuori di tale perimetro. In mancanza di un regime specifico, rimane quindi il problema di qualificare la responsabilità del certificatore privato che si avvalga di strumenti informatici o che partecipa insieme ad altri operatori come nodo di una blockchain. L'alternativa tra responsabilità contrattuale ed extracontrattuale del certificatore ritorna ad essere un problema rilevante nel dibattito dottrinale e non sono mancate le ricostruzioni che hanno

(30) È doveroso ricordare le considerazioni sviluppate a tal proposito da: M. S. Giannini, *Certezza pubblica*, in Enc dir., VI, 1960, Milano, 769.

(31) Sul punto cfr. F. Albisinni, *Certificazione dei prodotti agroalimentari e globalizzazione, tra concorrenza e tutela*, in *Rivista della regolazione dei mercati*, 2018, 20, secondo cui vi è "una peculiare sovrapposizione di ambiti disciplinari: privatistico quanto allo svolgimento delle attività in regime di concorrenza e di economicità di gestione e nel rispetto di contratti stipulati con le singole imprese controllate; pubblicistico quanto all'accreditamento, all'iscrizione nel registro degli organismi abilitati, alla designazione per le singole denominazioni, alle garanzie riconosciute alle imprese assoggettate a certificazione, alle finalità assegnate." Per una distinzione tra autoregolazioni "pure" (degli operatori e del mercato) e autoregolazioni completate da un intervento pubblico cfr. N. Rangone, *Declinazioni e implicazioni dell'autoregolazione: alla ricerca della giusta misura tra autonomia privata e pubblico potere*, in *Riv. dir. alim.*, n. 4-2011, 39.

(32) Per quanto riguarda i profili di responsabilità penale, va ricordato che è stato inserito nel codice penale l'art. 640-quinquies per reprimere le frodi informatiche del soggetto che presta servizi di certificazione di firma elettronica.

(33) Il decreto legislativo 26 agosto 2016, n. 179 ha modificato il codice dell'amministrazione digitale, introducendo alcune nuove disposizioni in riferimento soprattutto all'ambito di applicazione, alla firma digitale, all'armonizzazione con il diritto europeo.

rivista di diritto alimentare
www.rivistadirittoalimentare.it
Anno XIII, numero 1 · Gennaio-Marzo 2019

assimilato il servizio reso dal certificatore come un'attività da ricomprendere nell'ambito di applicazione dell'art. 2050 del codice civile[34], in considerazione dei delicati e complessi profili tecnici. Del resto, la giurisprudenza maggioritaria ritiene che non debbano essere considerate pericolose esclusivamente le attività elencate dal Testo Unico di Pubblica sicurezza, ma anche le attività, che per natura o per le caratteristiche dei mezzi adoperati, comportano rischi di danno valutabili mediante statistiche, elementi tecnici o secondo la comune esperienza, in termini notevolmente superiori rispetto ad altre situazioni ordinarie.

La direzione verso cui dottrina e giurisprudenza[35] sembrano muovere ha visto prevalere il criterio in base al quale le attività di certificazione[36] dei prodotti agroalimentari sono comunque assoggettate alle regole del mercato e della concorrenza, indipendentemente dalla natura, pubblica o privata, dell'ente certificatore.

A questo punto è veramente possibile semplificare tutti i problemi seguendo la tradizionale logica e applicando le categorie generali in tema di responsabilità civile oppure occorre una riflessione più matura, connessa a problemi inediti che sono il risultato delle nuove tecnologie?

Forse è arrivato il momento di cominciare ad esaminare i nuovi problemi, muovendo da prospettive differenti, perché ci troviamo di fronte a livelli di normatività inesplorata. Nell'ambito delle nuove tecnologie, gli esperti di informatica giuridica e di algoritmi contrattuali sono divisi tra chi ritiene possibile applicare gli strumenti giuridici elaborati tradizionalmente nell'ambito del diritto dei contratti e della responsabilità civile, e chi invece ritiene necessario riformulare elaborazioni concettuali *ex novo*[37].

È evidente che in materia esistono preoccupanti" lacune di responsabilità"[38], che sono inevitabilmente destinate ad aumentare in futuro senza un intervento di riorganizzazione e semplificazione normativa. Di fronte all'interrogativo della responsabilità dei controlli e dei dati affidati a computer in rete saremmo quindi in presenza di una lacuna difficile da colmare, considerando il complesso di azioni prodotte da computer connessi in rete l'uno

(34) La norma è stata richiamata dalla dottrina anche per il danno ascrivibile all'utilizzo nell'impresa alimentare di innovazioni tecnologiche. Tuttavia, questa ricostruzione non coprirebbe il "rischio da sviluppo" e quindi l'ipotesi in cui il danno alla salute sia provocato dal consumo di un nuovo alimento autorizzato in base alle conoscenze tecniche del momento e successivamente non confermate. L'impossibilità di configurare come difettosi nuovi alimenti autorizzati, ma comunque dannosi spinge la dottrina a riflettere in modo più adeguato sui profili di responsabilità degli operatori che utilizzano le nuove tecnologie. Per una riflessione approfondita su questi problemi cfr. M. Giuffrida, *Innovazione tecnologica e responsabilità dell'operatore del settore alimentare*, in *q. Riv.* www.rivistadirittoalimentare.it, n. 4-2018, p. 4 ss.

(35) Per un approfondimento della questione sulla distorsione della concorrenza causata dalle più ampie informazioni e dalle maggiori risorse delle Camere di commercio, rispetto agli organismi privati di certificazione cfr. TAR Lazio, sez. I, n. 11132/2015, nonché la Nota n. 10862 del 30 maggio 2016 dell'ICQRF (Ispettorato centrale della tutela della qualità e della repressione frodi dei prodotti agroalimentari), che accogliendo i rilievi giurisprudenziali e dell'Autorità Garante della Concorrenza e del Mercato, ha introdotto specifici obblighi procedimentali per gli organismi pubblici che operano nel mercato della certificazione dei prodotti agroalimentari. Per la ricostruzione della vicenda: Albisinni, *Certificazione dei prodotti agroalimentari e globalizzazione, tra concorrenza e tutela*, cit., 2018, nota 14.

(36) Per un approfondimento dei profili civilistici di certificazione e responsabilità del certificatore cfr. E. Bellisario, *Certificazione di qualità e responsabilità civile*, Milano, 2011, 261 s.; E. Bivona, *Le certificazioni di qualità: vizi del prodotto e responsabilità dell'ente certificatore*, in *Contr. impr.*, 2006, 1331 s.; A. Gentili, *La rilevanza giuridica della certificazione volontaria*, in *Europa e dir. priv.*, 1999, 59 s.; A. Luminoso, *Certificazione di qualità di prodotti e tutela del consumatore-acquirente*, in *Europa e dir. priv.*, 1999, 27 ss., G. Smorto, voce *Certificazione di qualità e normazione tecnica*, in Dig. IV, *disc. Priv. Sez. civ.*, Aggiornamento, I, Utet, Torino, 2003, 205 ss.

(37) Il dibattito tra i differenti orientamenti è sintetizzato da G. Teubner, *Soggetti giuridici digitali?*, Napoli, 2019, 20-21. Per l'orientamento favorevole ad una "riconcettualizzazione" dei problemi giuridici determinati dalle nuove tecnologie si veda in particolare G. Spindler, *Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?*, in *Juristenzeitung*, 2016, 805 s.; Id., *Zivilrechtliche Fragen beim Einsatz von Robotern*, in E. Hilgendorf (a cura di), *Robotik im kontext von Recht und Moral*, Baden-Baden, 2014, 63 s.

(38) L'espressione "lacune di responsabilità" è utilizzata da G. Teubner, op. cit., 26 per evidenziare che la dinamica della digitalizzazione produce spazi vuoti che le categorie giuridiche attuali non sono in grado di interpretare e comprendere in modo adeguato. L'A. menziona tra gli esempi di questa variegata casistica i computer in rete e i Big data, ritenendo che "fino a quando la dogmatica persisterà nel reagire alle nuove realtà digitali con lo strumentario concettuale tradizionale, continueranno ad emergere carenze nella disciplina della responsabilità". Per Teubner esistono in particolare tre rischi in materia di responsabilità derivanti dalla digitalizzazione: 1) il rischio di autonomia, nelle ipotesi di decisione prese direttamente dalla macchina; 2) il rischio di associazione, derivante dalla cooperazione tra uomo e agente software; 3) il rischio di interconnessione, che riguarda l'ipotesi di una pluralità di computer in rete. Id., op. cit., 37.

con l'altro e quindi in presenza di una responsabilità multipla che non potrebbe essere valutata adeguatamente in base alle sole norme vigenti in tema di responsabilità civile. Ulteriori "lacune di responsabilità" sono anche riscontrabili in tema di gestione di big data raccolti in base a calcoli rivelati errati "a monte".
Nelle more di soluzioni legislative più adatte a disciplinare le nuove fattispecie, si potrebbe però immaginare una responsabilità generale di impresa per i comportamenti illeciti derivanti dall'utilizzo delle nuove tecnologie. Il comportamento sarebbe quindi imputabile all'impresa che utilizza la tecnologia, fermo restando l'ipotesi di esenzione di responsabilità per "rischio da sviluppo", ma soltanto in caso di effettiva imprevedibilità del malfunzionamento tecnologico.

5.- Etichette intelligenti e Internet of things

Un'ulteriore riflessione è da fare per il sistema delle etichette c.d. "intelligenti" e per l'*Internet delle "cose"*. Lo sviluppo delle nuove tecnologie e l'introduzione di etichette in grado di rilevare alterazioni o pericoli per la salute in modo dettagliato potrebbe spingere, a pieno regime, a rivedere perfino i principi fondamentali che hanno fino a questo momento caratterizzato la politica dei controlli degli alimenti in Europa, rivedendo il ruolo di meccanismi basati sul principio di precauzione, in direzione di misure non più prudenziali e anticipate, ma azionabili in tempo reale, ed in grado di isolare e neutralizzare gli specifici problemi.
Ogni prodotto dovrebbe avere un'etichetta che permetta di leggere la sua storia e i passaggi da un operatore ad un altro.
Alcune piattaforme sono già in grado di utilizzare cryptosigilli per chiudere confezioni e imballaggi, evitando contaminazioni dei prodotti alimentari. Così, tra i vari esempi di applicazione delle nuove tecnologie in tema di packaging, possiamo ricordare, a titolo esemplificativo, il progetto cinese *WaBi* per realizzare "sigilli" anti-manomissione. Si tratta di codici criptati che possono essere letti tramite l'applicazione di uno smartphone, in grado di garantire la circolazione di prodotti sicuri. Il progetto è nato a seguito di uno scandalo avvenuto in Cina nel 2008 per l'alterazione di alcune partite di latte in polvere che aveva comportato la morte di bambini e numerosi intossicati. Il criptosigillo è in grado di rilevare qualsiasi manomissione durante il tragitto dallo stabilimento di produzione al consumo finale.
L'espressione Internet of Things (IoT o Internet delle Cose) indica il collegamento in rete tra oggetti, senza l'intermediazione dell'uomo ed in modo automatico. L'incorporazione di dispositivi informatici, quali chip a radiofrequenza (RFID[39]) consente la connessione. Tra le applicazioni dell'IoT occorre annoverare anche il sistema di etichette intelligenti. Tale sistema permette di realizzare dispositivi in grado di identificare e tracciare automaticamente le merci, permettendo letture multiple dei prodotti.
Il sistema non è soltanto in grado di tracciare i prodotti, ma anche di registrare le scelte dei consumatori, in quanto i *tags* dei RFID possono essere associati ai dati personali degli utenti. Sensori intelligenti possono aiutare a migliorare la salute delle persone o consentire la corretta conservazione degli alimenti, misurando ad esempio la temperatura o la contaminazione dell'ambiente circostante, evitando così il deterioramento degli alimenti. Si potrebbero monitorare più facilmente le scorte in magazzino, rilevando le quantità di merci acquistate e predisponendo un sistema in grado di evitare gli sprechi, consentendo in modo più razionale il consumo degli alimenti prima della loro scadenza o permettendo addirittura l'utilizzo degli stessi dopo che sia trascorsa formalmente la data indicata nella confezione del prodotto, qualora i sensori siano in grado di rilevare l'assenza di tossicità e quindi il possibile consumo

([39]) Con questa sigla si indicano microchip che contengono un codice identificativo che può essere letto in radiofrequenza. L'espressione *Internet of Things* è stata utilizzata per la prima volta da Kevin Ashton, presso il MIT (Massachussets Institute of Tecnology) per indicare oggetti in grado di connettersi ad Internet ed essere così sfruttati nella domotica e in moltissimi altri ambiti.

fuori termine. Tuttavia, l'utilizzo di sensori potrebbe comportare anche aspetti negativi, rivelando dati sensibili. Infatti, l'utilizzo di sistemi di radiofrequenza potrebbe essere applicato ad impianti sottocutanei, in grado di "intercettare" e selezionare gli alimenti più adatti alla tutela della salute di un determinato soggetto, o idonei a guidare le scelte di alimentazione promosse per ragioni etiche o convinzioni religiose. Per far fronte a questi inconvenienti, compatibilmente al Regolamento GDPR, dovrebbe essere sviluppato un sistema di "privacy by design", esaminando al momento della realizzazione dei sensori, l'impatto che la tecnologia è in grado di produrre in concreto rispetto alle esigenze di tutela della privacy. Quest'ultimo aspetto consente di rilevare che, parallelamente allo sviluppo di nuove tecnologie, non solo aumentano i vantaggi, ma anche i rischi per gli utenti, ed è evidente che il tema di un'adeguata protezione della sfera giuridica delle persone deve ancora essere approfondito dal punto di vista normativo, in modo più soddisfacente.
Questa riflessione permette così di aggiungere un altro argomento alla tesi della necessaria approvazione di uno specifico Regolamento in materia di e-privacy e di IoT[40], distinto dal GDPR[41].
Fino ad oggi, le uniche difese contro i rischi per la privacy connessi alle etichette "intelligenti", si sono limitate principalmente a mere raccomandazioni dirette a circoscrivere, quanto più possibile, le raccolte dei dati alle esclusive finalità previste per il loro trattamento, informando il consumatore sui rischi del sistema adottato, ma in futuro dovranno essere introdotte misure più efficaci e incisive rapportate ai nuovi pericoli di un governo dei Big Data, perché siamo entrati nell'era in cui è necessario tener conto che i vantaggi della tecnologia nascondono numerosi effetti collaterali che non sempre è possibile conoscere o prevedere.

ABSTRACT

The Blockchain can be used in the food trade, allowing to analyze and record all the steps from the producer to the consumer. The development of new technologies and the introduction of smart labels will be able to detect alterations or health hazards in detail. The new technology could be used to improve food controls, to provide information on ingredients and for many other purposes. The author shows, however, that there may also be disadvantages especially for the protection of privacy, so it would be desirable to have soon a regulation of new technologies.

□

([40]) In realtà, l'Unione europea ha approvato la Direttiva n. 2016/1148 (c.d. "Direttiva NIS" sulla Cybersecurity), ma si tratta di norme che purtroppo non sono al passo con il fenomeno descritto che avrebbe sicuramente bisogno di una regolamentazione più puntuale e completa.
([41]) L'art. 25 del GDPR in materia di protezione dei dati ricomprende sia i principi della "privacy by design", sia i principi della "privacy by default". Con il primo principio la protezione dei dati è integrata guardando all'intero ciclo della tecnologia utilizzata, dalla fase iniziale fino a quella finale, mentre il principio della c.d. "privacy by default" si ispira alle cautele generali di minimizzazione dei dati raccolti.