UNITÀ 5 CAPITOLO 1

Moneta elettronica e diritto alla riservatezza

La **moneta elettronica** è un tipo di moneta disponibile in forma digitale (anziché in forma fisica, come invece le banconote e le monete). Secondo l'art. 55, lett. *h ter* della legge n. 39 del 1° marzo 2002, attuativa della direttiva 2000/46/CE, la **moneta elettronica** è «un valore monetario rappresentato da un credito nei confronti dell'emittente che sia memorizzato su un dispositivo elettronico, emesso previa ricezione di fondi di valore non inferiore al valore monetario emesso e accettato come mezzo di pagamento da soggetti diversi dall'emittente».

Moneta elettronica, denaro elettronico, *e-cash*, *e-money* sono termini che hanno tutti lo stesso significato.

Un esempio tipico di moneta elettronica è il **borsellino elettronico**, chiamato anche **Smart Card**, da utilizzare per eseguire piccoli pagamenti. Si tratta di una carta prepagata e ricaricabile, dalla quale viene detratta di volta in volta la somma spesa per effettuare una transazione.

alexialex/iStock

La moneta elettronica può essere memorizzata ed utilizzata anche mediante dispositivi mobili o su internet con personali **account**. Quando viene utilizzato il termine "account" ci si riferisce, per esempio, ai **portafogli elettronici** che permettono ad un individuo di eseguire transazioni on line o in un negozio fisico attraverso l'uso di dispositivi elettronici come computer o smartphone.

L'utente accede al sito web della società che gestisce il sistema – il più noto è PayPal –, si registra gratuitamente e apre un proprio account con il quale può effettuare pagamenti utilizzando l'indirizzo e-mail e la relativa password. Al proprio account occorre poi associare un determinato metodo di pagamento, che può essere la propria carta di credito, a saldo o prepagata, oppure la carta emessa dallo stesso gestore del sito, ricaricabile senza spese dal proprio conto corrente bancario tramite bonifico.

La **moneta elettronica comprende la moneta digitale che non va confusa con la moneta virtuale**.

C'è differenza tra moneta digitale e moneta virtuale.

Nelle **monete elettroniche** la somma detenuta è espressa mediante la valuta avente corso legale, dunque vi è un rapporto diretto tra moneta elettronica e moneta reale: la prima è una pura dematerializzazione della seconda.

Nelle **monete o valute virtuali**, invece, l'unità di conto è essa stessa virtuale, dunque non è in diretto rapporto con la valuta avente corso legale.

La Banca centrale europea, nel 2012, ha definito la **moneta virtuale** una specie di moneta digitale **non regolamentata in nessuna giurisdizione**. Questo tipo di moneta viene rilasciata e controllata da sviluppatori indipendenti ed è utilizzata tra i membri di una specifica comunità virtuale. Nel 2014 l'Autorità bancaria europea ha chiarito che la moneta virtuale non ha legami con la Banca centrale o enti pubblici, ma può essere legalmente accettata in modo naturale tra persone che decidono di usarla come mezzo di pagamento.

ArtEvent ET/iStock

La moneta virtuale può essere trasferita, immagazzinata o scambiata elettronicamente. Ne sono un esempio i **bitcoin**. Si tratta di una moneta che non viene emessa da una Banca centrale, non viene stampata come la normale cartamoneta, ma viene creata, distribuita e scambiata in maniera completamente virtuale attraverso i computer e con una tecnologia *peer-to-peer*. Tale tecnologia, abbreviata anche come P2P, permette di creare una rete dove non esistono *server* e *client* esclusivi, poiché ogni dispositivo collegato è sia *client* che *server*, per cui tutti hanno la possibilità di **condividere con gli altri i dati presenti sul proprio computer**. Il bitcoin è una criptovaluta, cioè una valuta "nascosta", nel senso che è visibile/utilizzabile solo conoscendo un determinato codice informatico (le c.d. "chiavi di accesso" pubblica e privata, in linguaggio ancora più tecnico). I bitcoin vengono conservati all'interno di giganteschi *database* condivisi (ovvero fisicamente installati su più computer collegati tra loro alla rete internet) e attraverso sistemi avanzati di crittografia è possibile tracciarne le transazioni.

Altri strumenti elettronici di pagamento tra i più noti sono:

- le **carte di credito**, normalmente collegate a un conto corrente bancario intestato al titolare della carta. Con questo strumento è possibile effettuare acquisti di importi superiori alla disponibilità effettivamente presente sul conto. Il pagamento infatti è regolato dalla formula *pay later*, ossia l'addebito in conto avviene in un momento successivo a quello in cui viene utilizzata la carta. Le **carte di credito comuni** (dette "a saldo") consentono di posticipare l'addebito alla metà del mese successivo a quello in cui viene effettuato l'acquisto; mentre le **carte di credito revolving** permettono di dilazionare l'addebito in più rate. La principale differenza tra le due tipologie è dovuta quindi al momento in cui viene addebitata la spesa: con la prima viene speso del denaro di cui si è già in possesso, con la seconda invece viene spesa una cifra che si ipotizza avere disponibile in un prossimo futuro, ma di cui non si ha il possesso al momento dell'acquisto. L'addebito, pertanto, avviene nei termini e alle condizioni economiche stabilite nel contratto tra il titolare e l'emittente; nell'intervallo di tempo che intercorre tra l'acquisto del bene/servizio presso l'esercente di commercio convenzionato e l'addebito della somma sul conto corrente del titolare, l'emittente della carta (una banca o un intermediario finanziario) paga l'esercente di commercio per conto del titolare della carta e concede credito a quest'ultimo; ciò comporta per le carte di credito l'addebito di interessi passivi e costi più elevati rispetto alle carte di debito e alla moneta elettronica;
- le **carte di debito**, chiamate **bancomat**, ma impropriamente perché il termine "BANCOMAT" è un marchio registrato che identifica uno dei tanti circuiti utilizzati in Italia per il pagamento elettronico, tra cui "*Maestro*", gestito da *MasterCard*, e "*V-Pay*", gestito da *Visa*.

  Sono collegate a un conto corrente bancario intestato al titolare della carta sul quale vengono addebitate, al momento della transazione, le spese effettuate dal titolare del conto stesso. Anche nei casi in cui, per motivi tecnici, l'importo non venga addebitato immediatamente, l'emittente della

carta non concede credito al titolare della stessa: quando il conto corrente al momento dell'addebito non presenta un saldo sufficiente a coprire la spesa, il correntista si trova a pagare alla banca le spese previste dagli ulteriori contratti da lui firmati con la banca (interessi passivi del conto corrente, commissioni di massimo scoperto del fido, ecc.);

- le **carte prepagate** (ricaricabili e non). Esse prevedono che il titolare depositi una determinata somma all'intermediario finanziario emittente, effettuando poi i pagamenti fino a decorrenza di tale somma. Sono in genere utilizzate da chi non ha un conto corrente (come minori o studenti fuori sede, per esempio) o, soprattutto, da chi effettua acquisti on line o telefonici, in quanto il rischio di frode è limitato all'importo caricato sulla carta. Il pagamento viene addebitato istantaneamente: questa differenza sostanziale, con gli altri strumenti di pagamento è un rilevante vantaggio per chi deve incassare l'importo essendo garantito l'immediato accredito;
- la **carta conto**, **strumento di pagamento dotato di IBAN**, codice alfanumerico attribuito ai conti correnti, che **consente di eseguire molteplici operazioni come bonifici, domiciliazione utenze e ricariche ai cellulari**;
- il ***mobile payment***, con il quale è possibile effettuare pagamenti utilizzando dispositivi mobili come lo smartphone o il tablet. I pagamenti possono essere addebitati sul conto corrente, sulla carta di credito (a saldo o prepagata) o, comunque, con le modalità di pagamento che l'utente preferisce. Il servizio può essere attivato scaricando sul proprio dispositivo mobile l'apposita applicazione (in genere, gratuita) e registrando i propri dati personali e quelli dello strumento di pagamento che si intende utilizzare (carta di credito o prepagata, conto corrente bancario, borsellino virtuale ecc.). Per i pagamenti è previsto un PIN, che il titolare dovrà digitare per i pagamenti di importo superiore ad una determinata cifra di spesa;
- i **servizi di internet** o ***phone banking***, ossia i conti correnti aperti su internet (c.d. conti on line), i quali consentono al titolare di disporre pagamenti e trasferimenti di denaro a distanza, tramite l'uso di codici univoci e personali di identificazione; in questi casi, il servizio reso è solo un servizio di accesso a un deposito bancario.

PeopleImages/iStock

I pagamenti digitali si stanno diffondendo a macchia d'olio in molti Paesi del mondo con servizi mirati a semplificare la vita degli utenti. Tuttavia, questi nuovi strumenti di pagamento forniscono alle società che li gestiscono alcuni dati personali dei loro possessori, per cui gli utenti dei vari siti non sono più in grado di compiere transazioni in maniera anonima, come invece erano soliti fare utilizzando il denaro contante nel mondo reale.

Pertanto, sorge il problema della difesa del **diritto alla riservatezza**, un diritto fondamentale dell'individuo.

Nella **Costituzione italiana**, in quanto nata in un tempo in cui il diritto alla privacy non era sentito, non vi è un articolo specifico che tutela tale diritto, ma può essere ricavato per via interpretativa sia dagli articoli 2 e 3 della Costituzione stessa, che permettono di incorporare la riservatezza nei diritti inviolabili dell'uomo, sia dagli articoli 13, 14 e 15 Cost., nei quali si può cogliere la tutela della riservatezza in ambiti riguardanti la libertà personale, il domicilio, la libertà e la segretezza della corrispondenza e di ogni forma di comunicazione.

L'art. 12 della Dichiarazione universale dei diritti dell'uomo lo riconosce invece esplicitamente e recita:

«Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni.»

Il diritto alla riservatezza non è sinonimo di diritto "all'anonimato", ma è il diritto a mantenere il controllo sulle proprie informazioni quale presupposto per l'esercizio di molti altri diritti di libertà. Pertanto, lo Stato (e qualunque altro soggetto) deve astenersi dall'interferire in modo arbitrario o illegale nella vita privata della persona, ma, nello stesso tempo, deve accompagnare alla "astensione" anche la "protezione" di tale fondamentale diritto.

Non è facile perché si tratta di un diritto particolarmente complesso, in costante evoluzione, difficile ed esigente per una molteplicità di ragioni. Innanzitutto, in quanto coinvolgendo onore e reputazione, tocca la sfera più intima e sensibile della dignità umana, interpella cioè il valore dei principi dell'intera costruzione giuridica dei diritti umani, senza considerare poi il fatto che la diffusione via Internet di dati personali può indurre a comportamenti discriminatori o razzisti. Allo stesso tempo, la sua protezione (e la stessa interpretazione dei suoi contenuti) deve confrontarsi con l'evoluzione di una tecnologia sempre più pervasiva e invasiva e con le esigenze, sempre più impellenti, della sicurezza sociale e collettiva, interna e internazionale.

In futuro la partita si giocherà, allora, sulla diffusione e sull'implementazione di tecnologie che permetteranno la navigazione e lo svolgimento di operazioni nella rete con modalità meno invasive e meno rischiose per la privacy degli utenti.

Lo sviluppo di Internet, unito all'acquisita consapevolezza della pericolosa intrusività delle varie tecnologie adibite al tracciamento dei comportamenti e degli interessi degli utilizzatori della rete, comporterà l'adozione di protocolli, di software e di supporti fisici (per esempio le smart card) che siano in grado di rendere più sicuro e "anonimo" il navigare sulla Rete. Non solo, occorrerà affiancare ai provvedimenti a tutela della privacy efficaci strumenti di lotta alla

criminalità che sempre più sfrutta il contesto digitale per svolgere la propria attività illecita. Infine, occorre che ci siano appropriate normative sia a livello europeo, sia dei singoli Stati, che dispongano l'istituzione di appositi organi di garanzia e la messa in opera di adeguate procedure.

A **livello europeo e nazionale** il diritto alla riservatezza è oggi tutelato, in particolare:

- dal **Regolamento** (**Ue**) **2016/679** (nella versione inglese noto come **GDPR** – *General Data Protection Regulation*) del Parlamento europeo e del Consiglio europeo, del 27 aprile 2016, applicabile in tutti gli Stati membri, Italia inclusa, dal **25 maggio 2018**, relativo alla protezione delle persone fisiche, con riguardo al trattamento dei **dati personali** e alla libera circolazione di tali dati;
- dal **decreto legislativo 10 agosto 2018, n. 101**, che ha adeguato il Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del regolamento (Ue) 2016/679.

Per quanto riguarda i dati che un tempo si chiamavano **dati sensibili**, con l'entrata in vigore del GDPR hanno cambiato nome. Adesso sono **dati particolari**.

L'articolo 9 del GPDR ci dice che i dati particolari (ex-sensibili) non devono essere trattati, salvo consenso esplicito dell'interessato o in caso di necessità per assolvere ad alcuni obblighi ben codificati e indica come tali:

- l'**origine razziale o etnica**
- le **opinioni politiche**, le **convinzioni religiose o filosofiche**
- l'**appartenenza sindacale**
- i **dati genetici** e i **dati biometrici** intesi a identificare in modo univoco una persona fisica
- i **dati** relativi alla **salute** o alla **vita sessuale** o **all'orientamento sessuale** della persona.

Rispetto al **Codice della privacy italiano** (d.lgs. 30 giugno 2003, n. 196) nel **GDPR** è cambiata la forma, ma poco la sostanza. Ciò che è cambiato è il concetto stesso di dato personale, che sull'onda dell'evoluzione tecnologica è diventato qualcosa di più complesso rispetto a quello che veniva inteso una volta.

Pe3check/iStock

Oggi, per **dati personali** s'intendono tutte le informazioni che riconducono ad un singolo individuo attraverso le sue caratteristiche, relazioni, abitudini, stile di vita e così via.

Sono tali, pertanto:

- tutte le **informazioni identificative**, dai dati anagrafici alle immagini che ritraggono la persona;
- i **dati precedentemente definiti sensibili** e quindi sottoposti a tutela particolare;
- le **informazioni giudiziarie** che possono rivelare l'esistenza di determinati provvedimenti giudiziari a carico della persona;
- i **dati relativi alle comunicazioni elettroniche** via telefono o internet come, per esempio, un indirizzo IP;
- i **dati che consentono di geolocalizzare una persona** e da cui è possibile capire dove è andata, quando e a volte anche con chi;
- i **dati genetici e i dati biometrici**.

La Costituzione italiana ha pertanto bisogno di essere integrata, in via continuativa, da una più specifica normativa, nonché dalla giurisprudenza e dagli "interventi" (sanzionatori) del **Garante per la protezione dei dati personali** (Garante della privacy), autorità amministrativa indipendente.

Fonti

- blog.icard.com
- blockchain4innovation.it
- ecc-netitalia.it
- unipd-centrodirittiumani.it
- privacylab.it
- gdpr.net