Dianora Poletti

Il controllo dell'interessato nel mercato dei dati

1. Potrei iniziare il mio intervento con la fatidica frase: "C'era una volta il diritto al controllo dell'interessato sui propri dati personali" e svolgere le mie considerazioni rivolgendomi al passato. Tratterrò invece il tema guardando all'oggi, per verificare la sorte del controllo (quel che resta del controllo dell'interessato nella società della sorveglianza) e proverò a fare qualche riflessione con un occhio al futuro (come recuperare il controllo, se è possibile recuperarlo).

2. Non ci sono dubbi che il dibattito sulla protezione dei dati personali abbia ormai cambiato volto.

E' mutato profondamente in primo luogo l'humus della produzione dei dati. Da tempo superata è la configurazione in un rapporto circolare tra data subject e data controller che riguarda staticamente dati forniti "una volta tanto" e, per così dire, affidati dal primo al secondo. La connessione dei dispositivi in rete propria dell'IoT ci rende produttori continui di dati e inserisce le nostre informazioni in flussi di dati. Inoltre, i dati personali si mescolano ad altri dati (non personali, anonimi, ma anche dati misti, dati grezzi, dati inferiti, dati estratti e lavorati con le tecniche di data analisi), dando luogo a complessi reticoli di dati che richiedono l'interoperabilità dei sistemi, che a sua volta si coniuga con lo strumento del GDPR più proiettato al futuro: il diritto alla portabilità.

In secondo luogo, i dati, materia prima della economia digitale, sono entrati di necessità in questo mercato, tratteggiato con chiarezza dalla Strategia europea sui dati. Il fondamentale passo per la costruzione di un effettivo Mercato Unico Europeo postula l'impiego di regole relative alla libera circolazione di questi dati e alla loro condivisione, che devono conciliarsi: a) con il quadro regolatorio relativo ai diritti fondamentali, primi fra i quali quello alla protezione dei dati personali; b) con la tutela dei consumatori e di quanti utilizzano i servizi della società digitale rispetto all'uso dei dati che essi concorrono a generare attraverso la loro attività on line. Ecco perché si parla ormai di tutela multilivello o di approccio integrato, per indicare l'incrocio, non sempre facile da ricomporre, tra regole di data protection, di consumer protection e di concorrenza. La parola d'ordine, necessaria al funzionamento del mercato, è non più solo circolazione dei dati ma data sharing.

Terza ragione di cambiamento è l'affollamento del parterre di quelli che potremmo chiamare i soggetti del trattamento, che si è arricchito di nuovi personaggi: nel DGA sono comparsi gli intermediari dei dati, i "data holders" (titolari dei dati), ossia le persone giuridiche o le persona fisiche diverse dal data subject che, conformemente al diritto dell'Unione o nazionale applicabile, hanno il diritto (o l'obbligo) di concedere l'accesso a determinati dati personali o dati non personali o di condividerli con i "data users", cioè la «persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non

personali e che ha diritto, anche a norma del regolamento (UE) 2016/679 in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali".

La legge europea in fieri sui dati (la proposta di Data Act presentata nel febbraio scorso), che detta regole armonizzate per il corretto accesso e uso dei dati, non solo personali, inserisce in questo mercato i maggiori fornitori di questa mercanzia: i produttori di dispositivi connessi e i fornitori di servizi correlati.

Non ultimo, anche il data subject ha cambiato la sua identità, posto che è divenuto ormai sempre di più un "agente legittimante" dell'ulteriore circolazione dei suoi dati, senza contare che nella Privacy Group non rileva più come soggetto da identificare necessariamente, ma come soggetto accomunato ad altre collettività da preferenze di consumo e non solo.

3. In questo contesto, mutato e reso oltremodo complesso, cosa resta del principio-guida del controllo dell'interessato e come lo stesso può continuare ad essere esercitato con un minimo di effettività in un ecosistema nel quale la costante circolazione dei dati tra diversi operatori fa perdere al data subject la possibilità di conoscere quali soggetti stiano compiendo attività di trattamento e in cui si registra l'ulteriore perdita di efficacia del consenso?

Per ragioni di tempo devo limitarmi a un cenno fugace al Data Act e a uno – appena un po' meno fugace) al Data Governance Act.

4. In che veste emerge nel nascente Data Act il controllo dell'interessato? Il data subjet è beneficiario di una serie di obblighi che vengono posti in capo ai data holders. Quando vengono trattati dati personali, il data holder è considerato un responsabile del trattamento e deve fornire informazioni sui dati che saranno generati quando si utilizza il prodotto o il servizio, compresa la natura, il volume dei dati e da chi e come l'utente può richiedere che questi dati siano condivisi con una terza parte. Il data subject può anche coincidere con il "data user", considerando che nella nozione di data user è compresa la persona fisica che possiede, noleggia o prende in leasing un prodotto o riceve un servizio (come per esempio la persona fisica utilizzatore di smart assistant o di prodotti domotici).

Nel contesto del governo dei dati derivanti dai prodotti connessi, il supporto all'effettività del controllo dell'interessato è riservato alle informazioni che fino ad oggi mancavano: quali siano questi dati, chi li utilizza e come l'utente può accedervi. Si prova così a colmare il profondo gap informativo dell'interessato - spesso all'oscuro del trattamento - di fronte ad un prodotto o a più prodotti connessi e interoperabili. È però chiaro che la circolazione del dato nel Data Act (nel quale – non dimentichiamocene – i dati personali sono solo uno spicchio del regolato e nel quale è nitida la vocazione commerciale) è una questione che riguarda prevalentemente i data holders e i data recipients (risépients), cioè coloro che svolgono attività imprenditoriale o commerciale, ossia chi ha la capacità di rendere disponibili i dati (specie non personali) e chi intende sfruttarli.

5. Come è invece conformato il controllo del *data subjec*t nel DGA?

Semplificando al massimo, in questo regolamento rinveniamo un quadro regolatorio per la fornitura di servizi di intermediazione dei dati, posto che lo stesso si propone di disciplinare l'attività degli intermediari dei dati, ossia dei fornitori dei servizi di condivisione dei dati personali, il cui ruolo viene considerato essenziale dall' UE, e comprende nel suo ambito di applicazione proprio i fornitori di servizi di intermediazione tra un numero indefinito di persone interessate e un numero indefinito di potenziali utenti dei dati.

Il DGA disciplina l'attività di questi soggetti introducendo meccanismi di controllo, come un sistema di notifica obbligatorio all'autorità competente nazionale e una serie di obblighi e requisiti posti in capo ai fornitori di servizi di condivisione di dati, volti a scongiurare un uso improprio dei dati trattati, a delineare il loro ruolo neutrale rispetto ai dati scambiati tra gli utenti e a garantire la loro posizione indipendente tanto dai titolari dei dati quanto dagli utenti degli stessi, realizzando una separazione anche strutturale del modello organizzativo dell'attività di impresa.

Trapela però dal regolamento anche un orizzonte differente, che appare di sicuro rilievo per il controllo dell'interessato, perché agli intermediari dei dati è attribuito anche il compito di esercitare i diritti degli interessati in relazione ai dati personali. Una categoria specifica di fornitori di servizi di intermediazione dei dati comprende proprio i fornitori che offrono i loro servizi agli interessati. Tali fornitori di servizi di intermediazione dei dati dovrebbero rafforzare la capacità di agire degli interessati e, in particolare, il controllo dei singoli individui in merito ai dati che li riguardano attraverso attività di tipo consulenziale.

Questo è particolarmente evidente nel punto del regolamento in cui si prevede i fornitori di servizi di intermediazione possono assumere anche la veste di cooperative di dati, le quali dovrebbero mirare a rafforzare la posizione dei singoli individui affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati. Si legge nel regolamento che l'attività delle cooperative si dirige ad aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compimento di scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali.

Viene in questo modo cristallizzato un modello, per vero già registrato nella prassi, basato sul ruolo degli intermediari di dati (infomediari) che fungono da "centri di raccolta" di dati personali forniti direttamente dagli utenti, che possono esercitare loro tramite, con un mandato di natura fiduciaria, i propri diritti e controllare direttamente come e a quali terzi concederne l'utilizzo, non escluso a fronte di una remunerazione.

La constatata debolezza dell'interessato nell'esercizio del suo diritto al controllo legittima una sua sostituzione attraverso la legittimazione rappresentativa di soggetti che perseguono finalità non egoistiche. Non vi è dubbio che a questi intermediari possa essere attribuita la gestione dei diritti dell'interessato, forse già a partire dal rilascio e dalla revoca del consenso al trattamento dei dati, sicuramente per l'esercizio dei diritti riconosciuti dal GDPR.

Emerge con decisione, di fronte al data subject sempre più solo di fronte agli operatori del mercato dei dati, l'esercizio delegabile dei diritti, la configurazione di un rapporto gestorio e fiduciario tutto da costruire (ben oltre la figura del mandatario già noto per la gestione l'eredità digitale previsto dall'art. 2 terdecies del codice della privacy). Non si può non ricordare al riguardo l'art. 80 del GDPR, secondo la quale la tutela dei diritti dell'interessato può essere reclamata anche da un ente legittimato, anche in assenza di un mandato a tal fine ma – aggiungerei – anche l'art. 13 della prima legge italiana in materia (la 675/1996) che già prevedeva (con una scelta poi lasciata impropriamente cadere negli aggiustamenti successivi) che, nell´esercizio dei diritti (incluso quello, strumentale agli altri, del controllo) l´interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

6. Se per recuperare effettività al controllo è necessario attrezzarci diversamente dal passato, sembra possibile pensare anche "il riuso per il controllo dell'interessato di strumenti nati con finalita' altre".

È questo il caso della Blockchain. Superata la fase iniziale di analisi della difficile convivenza della BC con il GDPR, le più mature riflessioni sul tema si sono dirette a immaginare soluzioni in grado di riconciliare quello che appariva incompatibile.

Non ho il tempo di approfondire e di addentrarmi in tecnicismi sui modi in cui si può comunque consentire di non mettere in chiaro l'informazione personale su BC, ma voglio porre l'accento sul fatto che la tecnologia *blockchain* favorisce *in re ipsa* l'integrità e la sicurezza dei dati, garantendo la correlata resistenza ad eventuali attacchi esterni, per il fatto che tale tecnologia conserva la memoria storica delle transazioni in modo immutabile e garantisce a ciascun partecipante una copia di ciascuna operazione.
La BC potrebbe allora essere ripensata un arnese impiegabile dall'interessato per il recupero del controllo sui propri dati. Proprio nella prospettata *governance* europea dei dati, anche in forza della possibile "riconciliazione" con il GDPR, la *blockchain* emerge con la veste di strumento utilizzabile non solo dalle imprese per rafforzare la loro presenza nel mercato digitale, ma anche dai *data subjects* per recuperare il diritto al controllo sui propri dati.

Questa potenzialità della *blockchain* è dichiarata dalla Risoluzione del Parlamento europeo sulla *blockchain* e i registri distribuiti del 2018, che si pone come primo obiettivo il fatto che le tecnologie 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 sfruttare tali dati.

Nel mercato sono da qualche tempo in essere esperimenti e applicazioni nelle quali la *blockchain* è utilizzata con questi obiettivi (attribuire all'interessato il controllo sulla direzione dei flussi di dati che genera e la scelta dei soggetti con i quali condividere gli stessi). Tale possibilità emerge espressamente dalla Strategia europea per i dati, che richiama, per fornire alle persone fisiche i mezzi per decidere di volta in volta in dettaglio come sono utilizzati i loro dati, strumenti per la gestione del consenso, *app* per la gestione delle informazioni personali, ma anche «soluzioni completamente decentrate basate sulla *blockchain*».
Mutuando da esperienze applicative già in atto nel nostro Paese, i flussi di dati provenienti dai sensori e oggetti intelligenti potrebbero essere scambiati utilizzando mercati online di dati che consentono all'interessato di mantenere il controllo sui propri dati, attraverso gli Smart Contracts.
Ambienti tecnologici così congegnati possono riattribuire nuova pregnanza proprio al consenso e rafforzare l'efficacia della sua revoca. In ogni momento, infatti, l'interessato (che è a conoscenza di chi utilizza i suoi dati) può revocare il consenso, sempre tramite lo *smart contract* che provvederà a "chiudere" il flusso dei dati.
Un design di questo tipo – che combina BC e SC - può realizzare obiettivi di *data sharing* in maniera decisamente più controllata (e anche GDPR-*compliant*) di quanto accade comunemente. Soluzioni come queste – magari poste in essere tramite i nuovi intermediari dei dati del DGA - potrebbero realizzare una sorta di "*consumer empowerment*" e fare partecipare al processo, come soggetto attivo, lo stesso interessato.

7. Una breve notazione per concludere.

Nell'economia dei dati il diritto al controllo diventa sempre più difficile da esercitarsi (con il linguaggio europeo, diremmo sempre meno effettivo) e quindi deve essere diversamente ricostruito, perché ha bisogno di sostegni esterni.

Diventa così un controllo delegabile, supportato, intermediato, anche incorporato nella tecnica, che si pone al centro di nuovi rapporti contrattuali (quello che lega l'interessato all'intermediario, per esempio) che fuoriescono dall'originaria relazione dell'interessato con il titolare, può assumere persino una dimensione di esercizio collettivo in forma di legittimazione rappresentativa quando l'interessato si affida ai nuovi servizi di intermediazione dei dati.

Spetterà al lavorio dell'interprete dipanare al meglio tutti grumi di problematicità che lo circondano, e allo studioso privatista in particolare ripensare a un efficiente uso di strumenti negoziali per consentire al data subject, all'interno di una rete complessa di operatori e di rapporti negoziali, diciamolo pure, anche mercantili, di non perdere il diritto di "inseguire" il dato che lo riguarda.