"La nuova emergenza per la privacy mondiale si chiama app economy" - Intervento di Antonello Soro

La nuova emergenza per la privacy mondiale si chiama app economy

I limiti e i rischi di un sistema commerciale in cui le condizioni generali di contratto, unilateralmente stabilite dalle aziende del digitale, finiscono con il definire il perimetro dei diritti e delle libertà

Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali

("Il Foglio", 12 gennaio 2019)

Al direttore - L'"App economy" è uno dei settori del sistema economico attuale in maggiore espansione, che oggi impiega 1,8 milioni di persone solo in Europa e il cui valore, in termini di fatturato, si stima cresca esponenzialmente nei prossimi anni. Ma possiamo considerare l'espressione "app economy" anche come una delle più appropriate definizioni dell'economia digitale, in cui una parte significativa degli scambi commerciali è veicolata attraverso applicazioni scaricate dai consumatori, per i fini più vari, su smartphone, tablet ecc. Nella maggior parte dei casi, le app forniscono servizi gratuitamente o, meglio, richiedendo un corrispettivo non patrimoniale: i dati. Essi sono utilizzati per costruire profili di consumatori utili a indirizzare efficacemente l'attività di marketing e rappresentano, quindi, tanto un bene rilevante dal punto di vista economico, quanto l'oggetto di un diritto fondamentale. All'interno delle innumerevoli tipologie di applicazioni offerte dal mercato digitale, proliferano recentemente quelle che consentono di ottenere informazioni sull'intestazione dei numeri digitati, attingendo a una banca dati alimentata dagli utenti stessi, che vi inseriscono i contatti della propria rubrica. Si pensi, ad esempio, a Sync.Me. Il funzionamento di queste applicazioni – i fornitori delle quali sono stabiliti spesso in Paesi extraeuropei – suscita riflessioni interessanti, tanto sul caso singolo quanto di sistema. Per quanto riguarda i profili privacy, vorrei segnalare una serie di criticità. Anzitutto, rispetto ai limiti del consenso. Anche ipotizzando che esso sia effettivamente acquisito, ci si deve chiedere se sia realmente informato e dunque se l'utente abbia effettiva consapevolezza dell'uso che dei dati conferiti sarà fatto. In assenza di un'informativa adeguata, infatti, il consenso stesso non potrebbe ritenersi validamente prestato, con le conseguenze che ne derivano in termini sanzionatori e di inutilizzabilità delle informazioni così acquisite. E se tutto questo riguarda i limiti del consenso dell'utente al trattamento dei propri dati, ulteriori criticità solleva il tema della cessione dei contatti della rubrica. Di questi l'utente non può validamente disporre – cedendoli a un fornitore che li utilizzerà in un contesto commerciale – in assenza del consenso del terzo. Questa circostanza evidenzia i limiti e i rischi di un sistema commerciale in cui le condizioni generali di contratto, unilateralmente stabilite dalle aziende del digitale (o dai big tech con innumerevoli "terze parti"), finiscono con il definire il perimetro dei diritti e delle libertà. Ed evidenzia come – spesso inconsapevolmente – gli stessi utenti si rendano vittime e ad un tempo autori di illeciti, lasciando che non soltanto i propri dati, ma anche quelli di terzi, siano utilizzati come merce preziosa (ma a costo zero) da parte delle aziende del digitale.

Gli utenti devono essere consapevoli di come la cessione di informazioni relative ad altre persone, in assenza del loro consenso, costituisca un illecito sanzionato anche gravemente. E, per quanto concerne la cessione dei propri dati, in cambio delle piccole o grandi utilità fornite dalle app, devono essere consapevoli dei rischi (in termini di furti di identità, accessi abusivi, ecc.) propri di un simile sistema commerciale, che si alimenta della monetizzazione di quei preziosi frammenti di libertà che sono le informazioni personali.

Vi è poi da considerare l'impatto geopolitico e sull'assetto e la trasparenza del mercato, proprio di simili sistemi commerciali, con aziende localizzate prevalentemente al di fuori dell'Unione europea e in veri e propri paradisi dei dati, assai più sfuggenti e "sommersi" di quelli fiscali. E, forse, anche più pericolosi, se si considera che nella dimensione digitale si dispiegano oggi le ostilità tra soggetti, tra Stati e tra "blocchi" di nazioni e poteri. Ora, sotto il profilo della privacy, la localizzazione extra-europea non sarebbe ostativa all'applicazione del GDPR, per la quale è sufficiente l'offerta di beni o servizi a persone che si trovino nell'Ue. Questa circostanza non impedirà dunque alle Autorità di protezione dati europee di condurre attività istruttorie e se del caso anche sanzionatorie. Resta tuttavia l'innegabile difficoltà dell'esecutorietà di tali provvedimenti, rispetto a soggetti verso i quali, in caso di

inadempimento, risulta alquanto problematico non solo ricorrere alle sanzioni penali previste in caso di inosservanza, ma anche più banalmente realizzare efficacemente attività ispettive. Per superare queste aporie è indispensabile il riconoscimento, a livello internazionale, del diritto alla protezione dei dati personali e delle garanzie necessarie per assicurarne l'effettività. In un contesto globale come quello della rete, fondato sull'interdipendenza e sul superamento di confini e frontiere, la tutela dei diritti non può che essere altrettanto globale e basata su livelli omogenei di garanzia.