IL DIRITTO INTERNAZIONALE NELL'ERA DELL'*INTERNET OF THINGS*: BIG DATA E TUTELA DELLA PRIVACY

SABRINA PALANZA

DIPARTIMENTO DI SCIENZE POLITICHE, A.A. 2015/2016
CDL: RELAZIONI INTERNAZIONALI
RELATORE CARLO FOCARELLI

VINCITRICE DEL PREMIO DI LAUREA ALFREDO DE POI

Negli anni a venire saremo sempre più "connessi" gli uni con gli altri e, soprattutto, con il resto del mondo (oggetti compresi) che ci circonda. Questa incredibile rivoluzione viene spesso indicata con l'espressione "Internet of things" (IoT), coniata nel 1999 dal ricercatore britannico del Massachussets Institute of Technology (MIT), Kevin Ashton. L'identificazione di ciascun oggetto avviene tramite piccoli sensori, *Tag Rfid* o attuatori che sono applicati agli oggetti, affinché questi trasmettano e ricevano informazioni, utilizzando come piattaforma di scambio il web, nella quale, in un secondo momento, vengono archiviati/memorizzati e rielaborati i dati raccolti (e "trasformati", quindi, in *big data*) provenienti, dunque, dal mondo fisico circostante. Estensioni dell'IoT, anche se non parte del concetto originale, sono l'*ambient intelligence* e l'*autonomous control*: la prima indica un ambiente costituito da oggetti che rispondono alla presenza di esseri umani agendo in conformità a determinate aspettative di questi; la seconda amplia il campo d'azione applicando strumenti intelligenti a ciascun oggetto reale o virtuale e mettendoli in grado di comunicare tra loro.

L'*Internet che vive nelle cose* cambierà, e sta già cambiando, profondamente le nostre vite, trovando applicazione in diversi ambiti: dalla sanità alle *utility*, dalla produzione alla pubblica amministrazione; IoT vuol dire "integrazione", secondo diversi esperti, e aprirà, per esempio, importantissime prospettive in termini di rivisitazione dei sistemi informativi aziendali. Anche da questo punto di vista questa tecnologia rivoluzionaria, rappresenterà un'importante occasione di sviluppo. Una marea di dati, quindi, che fluiscono da un oggetto *smart* ad un altro, o verso altri utenti, passando per il *cloud* e che diventano il "carburante" che ogni singolo individuo produce, quasi sempre, consapevolmente. Mentre, quindi, i dispositivi *smart* , da un lato, promettono benefici ed semplificazioni delle attività quotidiane che ognuno di noi deve svolgere, dall'altro introducono una serie di nuovi rischi e pericoli per la sicurezza e la privacy del singolo individuo, che *sceglie* di cedere i suoi dati in cambio di questi servizi. Basti pensare a possibili attacchi hacker, furti d'identità online, accesso ai dati personali da parte di malintenzionati, raccolta di dati di qualsiasi tipo per fini secondari (quindi anche "sensibili", ad oggi tutelati dalle normative vigenti) da parte di imprese multinazionali con relativo e successivo controllo della produzione, processo che modificherebbe, di conseguenza, il sistema economico finora conosciuto. Quest'elenco, infine, termina con ciò che forse per alcuni risulterà ancora *fantascientifico* ma che, in realtà, come sostengono autorevoli esperti in materia, è tutt'altro che "hollywoodiano": il controllo del comportamento umano, dettato da una società composta da individui che si "sorvegliano reciprocamente" e nella quale non sono ammesse "diversificazioni"; la c.d. automazione sociale.

Delineato lo *stato dell'arte* e i possibili scenari futuri, la domanda alla quale si è cercato di rispondere nell'elaborato, presa consapevolezza della complessità e della vastità dell'oggetto in analisi, è stata: cosa si chiede al diritto, e nella fattispecie, al diritto internazionale? Quale sarà il "futuro del diritto" o il "diritto del futuro"? Attraverso un'analisi quanto più aggiornata delle linee guida delle Nazioni Unite, raccomandazioni e pareri provenienti dai più autorevoli organi internazionali, si è giunti alla conclusione che la produzione

giuridica attuale non sia ancora in possesso di strumenti adatti alla gestione di un fenomeno così *globale* e di portata rivoluzionaria, e quindi, gli organi internazionali risultano essere lontani dalla promulgazione di norme valevoli ovunque. Una delle cause di ciò risiede nelle diverse concezioni di "privacy" esistenti, rilevata attraverso un *focus* specifico sullo *status quo* negli Stati Uniti e in Europa, attraverso un approfondimento della recente prassi in materia di protezione dei dati e privacy (le sentenze della Corte di Giustizia dell'Unione europea, *Google-Spain* e *Maximillian Schrems v. data protection*, che hanno portato all'invalidamento del *Safe harbor*). Questa differenza concettuale di matrice *storica* e *culturale*, infatti, ha fatto sì che la produzione legislativa nazionale (o macro-regionale) risulti essere ancora scissa tra un sistema europeo "ancorato" al rispetto dei diritti umani, ed un sistema americano più frammentato e volto al raggiungimento del profitto economico.

Auspicando, quindi, un avvicinamento di questi due modelli, volto a favorire la crescita tecnologica senza rinunciare al rispetto dei diritti umani, e convivendo quanto espresso da parte della dottrina, abbiamo ritenuto che la "modernizzazione" della Convenzione n. 108 del 1981 che, grazie all'art. 23 è aperta anche all'adesione di paesi extra europei, avvicinerebbe la sfera normativa in questione allo scenario economico e tecnologico attuale, incentivando i Paesi a farne parte per non perdere la fetta di mercato europeo. Del resto, il diritto non può non tener minimamente conto del fattore economico, che oggi risulta essere molto importante per lo sviluppo tecnologico, prevedendo altresì norme che vadano a scoraggiare eventuali investimenti in alcune aeree del mondo a causa di un impianto giuridico troppo "paralizzante" e superato. A nostro avviso, infatti, le norme giuridiche nel mondo *2.0* devono parlare, in ultima istanza, alla collettività mondiale e non più esclusivamente a quella regionale, favorendo un'omogeneizzazione normativa per la raccolta e il trattamento dei nostri dati, che data la vastità della Rete, non vengono quasi mai trattati nel paese, o addirittura nel continente, di residenza dell'utente.

Regolamentare il processo produttivo degli oggetti *smart*, individuando responsabilità (e dunque diritti e doveri) e *status* giuridico delle varie figure coinvolte nel *patchwork* dell'IoT (dal produttore al designer, passando per il fornitore dei software), abbondare l'impostazione "dato-centrica" di cui la Corte di Giustizia dell'Unione europea finora si è servita per le sue pronunce ed iniziare a chiedersi se la nozione di privacy, e quindi di "vita privata", così come prevista, per esempio, dalla Dichiarazione universale dei diritti umani e dalla Convenzione Europea dei diritti dell'uomo, debba essere ripensata alla luce di un'evidente difficoltà nell'individuare il confine vigente tra "luogo pubblico" e "luogo privato", a causa di una tecnologia che *annulla le differenze*, potrebbero essere, a nostro avviso, alcuni dei punti di partenza per rispondere alle domande che ci hanno spinto alla stesura di questo elaborato.