

Il diritto e il mondo informatico

Il mondo odierno è sempre più caratterizzato dall'uso frequente di sistemi informatici che mettono in contatto tra loro milioni di persone ogni giorno, disperate in tutto il globo, attraverso l'uso di *internet* e i *social network*.

Secondo il dr. Gary Small, un ricercatore dell'Università della California, navigare in rete ha un'azione positiva sul cervello; si è constatato che utilizzare internet per cercare qualcosa, può aumentare memoria e capacità decisionali, allenando determinate aree del cervello.

Al tempo stesso, la rete può risultare un'arma a doppio taglio con la quale si possono mettere a rischio la propria *privacy*, il *copyright*, la *dignità personale* mediante *diffamazioni*, *truffe* ma perfino essere soggetti di un *attacco informatico*.

Il diritto, in continuo fermento ed evoluzione, cerca di disciplinare la materia per dare risposte certe e tutele concrete, in questa tematica di non facile interpretazione: molti autori, in questo specifico caso, parlano di *diritto versione 2.0*, in analogia all'evoluzione del *web*.

Quando il singolo *utente* è connesso su internet alla ricerca di informazioni, lo si aggettiva comunemente come persona che *naviga* o *surfa* sul web. Nell'immaginario collettivo invece il *pirata* è visto come colui che con una gamba di legno ed una benda sull'occhio, un pappagallo sulla spalla, commette crimini e reati, al capo di un vascello, con il solo scopo di illecito arricchimento. Riportando tale concetto di pirata in un contesto tecnologico, possiamo figurare il pirata informatico che, usando il suo vascello come *computer*, naviga per mari di *internet*, abbordando e depredando l'ignaro *surfista di internet*, privandolo dei suoi diritti.

La risposta normativa europea a tali atti illeciti, non si è fatta attendere.

In particolare in Ungheria e per la precisazione a Budapest, è stata firmata in data 23 novembre 2001, la Convenzione del Consiglio d'Europa sulla *criminalità informatica*, accompagnata da un Protocollo aggiuntivo relativo alla criminalizzazione degli atti di natura razzista e xenofoba commessi attraverso l'uso di sistemi informatici.

Tale convenzione, entrata in vigore nel 2004, in un'ottica di completezza, di recente ha concentrato la propria attenzione sul versante delle garanzie atte ad assicurare anche nel mondo virtuale il godimento dei diritti pacificamente riconosciuti nella Convenzione Europea dei diritti dell'uomo. Sotto il profilo procedurale, la Convenzione indica misure di accertamento e di repressione dei crimini informatici che in parte si rifanno ad istituti tradizionali adatti alla realtà virtuale (sequestro e perquisizione), in parte consistono in misure specifiche come la raccolta e la conservazione rapida dei dati informatici, atte a superare il problema della volatilità delle prove, tipiche della attività virtuale. È prevista poi la cooperazione internazionale tra Stati, basata su assistenza ed estradizione.

Con il passare del tempo, sul filone dell'armonizzazione della materia, con il Trattato di Lisbona del 2009 viene inserito il concetto di “*criminalità informatica*” nell'art. 83 TFUE fra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione Europea ha competenza penale.

Gli Stati membri sono chiamati a punire come reato l'accesso illecito a sistemi di informazione, la interferenza illecita per quanto riguarda i sistemi e i dati; l'intercettazione illecita nonché la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, il possesso, la messa a disposizione in altro modo di specifici strumenti utilizzati per commettere i reati, sempre che i suddetti abbiano agito dolosamente.

Devono considerati reati anche l'istigazione, il favoreggiamento, la complicità e il tentativo.

La determinazione delle sanzioni, è lasciata alla discrezionalità degli Stati.

In merito alla competenza giurisdizionale, i criteri risultano essere quelli tradizionali della territorialità (il luogo della commissione del delitto) oppure la nazionalità o la residenza abituale dell'autore del reato o la sede legale della persona giuridica. Su questo punto, ad oggi resta aperta la questione e la difficoltà di individuare concretamente il luogo esatto in cui avviene il reato e/o identificare l'autore materiale del reato.

Per ultimo, a fronte dei recenti attacchi terroristici è stato istituito in data 11 gennaio 2013 presso l'Europol (*European Police Office, Ufficio di Polizia Europeo*) un Centro europeo contro la criminalità informatica, lo EC3 (*European Cybercrime Centre*) con l'intento di creare un nodo di collaborazione e cooperazione per la difesa di uno spazio virtuale, libero ed aperto.

Per concludere,
auguro a tutti una felice e sicura navigazione online.

dr. Amato Lorenzo
in collaborazione con **Studio Legale Avv. Bálint Halmos**