



Privacy e Safe Harbour: a inizio 2016 la fine del mondo?

Le istituzioni europee hanno poco tempo per trovare un accordo con gli Stati Uniti

Sullo scorso numero di *PC Professionale* (e sul sito della rivista) ho commentato la sentenza del 6 ottobre 2015 con la quale la Corte di giustizia europea ha annullato l'accordo fra Europa e Stati Uniti sullo scambio di dati personali fra i due continenti. E che, di conseguenza, ha lasciato senza copertura legale migliaia di imprese che hanno fatto affidamento su questo strumento giuridico per condurre le loro attività. All'indomani della sentenza, la situazione si è aggravata perché sia il Gruppo di Lavoro Articolo 29 (sostanzialmente una sorta di "autorità di protezione dei dati personali europea"), sia alcuni garanti nazionali (primi il tedesco, poi il portoghese e da pochissimo quello italiano) non hanno ritenuto di aspettare l'esito dei negoziati euro-americani e si sono affrettati a dichiarare illegale lo scambio di dati basato sul (defunto) Safe Harbour. Chi sperava che con il passare del tempo la situazione si normalizzasse e che, con un po' di buon senso, fosse possibile raggiungere una soluzione in breve tempo è rimasto deluso.

Evidentemente, la Corte di giustizia europea, il Gruppo di lavoro Articolo 29 e la Commissione europea stanno seguendo ciascuno una propria agenda, non necessariamente sincronizzata con quella degli altri. La prima ha evidentemente

deciso di "fare la storia" in materia di diritti digitali, emettendo delle sentenze, come quelle sul diritto all'oblio, sulla data-retention e sul Safe Harbour che condizioneranno le istituzioni europee negli anni a venire.

I Garanti, dal canto loro, hanno improvvisamente scoperto (super)poteri di controllo che avevano casualmente dimenticato di avere e che ora annunciano di voler esercitare a partire dal prossimo gennaio 2016, se Europa e Usa non avranno trovato un accordo soddisfacente.

La Commissione naviga a vista in uno stretto, senza una rotta definita, costretta a subire i colpi di Scilla (la Corte) da un lato e Cariddi (i Garanti dei dati personali) dall'altro. E senza avere nulla di sostanziale da dire alle sue controparti americane, come ha confermato l'incontro di metà novembre fra il Commissario europeo alla giustizia Jourova e il Department of Commerce. A questo, va aggiunta la contingenza dell'attentato di Parigi che ha fortemente indebolito le posizioni dei difensori della privacy, e ben difficilmente almeno in questa fase la Commissione potrà sponsorizzare misure che limitano le

capacità di prevenzione e reazione contro il terrorismo.

Il risultato pratico è che, per rimanere nella metafora militare, il controllo del bottone che fa partire raffiche di ispezioni e controlli è nelle mani dei Garanti dei dati personali. E a quanto pare costoro sono intenzionati a premerlo se non verranno raggiunti accordi soddisfacenti.

Certo, sarebbe anche astrattamente possibile che, giunti al punto di non ritorno, i Garanti decidano di non agire. Lo hanno già fatto nel caso dell'abrogazione giudiziaria della direttiva sulla data-retention, che imponeva loro quantomeno di rivedere la legittimità delle normative nazionali di settore sulla conservazione di massa dei dati degli utenti. E lo hanno rifatto con l'applicazione della "direttiva cookie", imponendo obblighi meramente formali, come il ridicolo "cookie banner" che campeggia oramai dappertutto e che a tutto serve tranne che a tutelare gli utenti. Se tuttavia, nel groviglio di posizioni e interessi politici spesso confliggenti, questa potrebbe effettivamente essere la soluzione più pragmatica, proprio per questo è la meno probabile. Dunque le imprese non solo ICT dovranno innanzi tutto rivedere profondamente i propri modelli commerciali cercando di limitare al massimo il trattamento dei dati personali che vengono eventualmente trasferiti oltreoceano e poi dovranno

mettere in conto di dover affrontare i costi derivanti dalle sanzioni dei Garanti e quelli necessari per impugnarle davanti alla magistratura ordinaria. Anche se, a onor del vero, bisogna dire che i soggetti più a rischio sono i titolari di piattaforme (Facebook, Google) la cui attività si basa

essenzialmente sulla profilazione degli utenti. Per una volta, dunque, l'incapacità e l'arretratezza delle internet company italiane si è dimostrata un vantaggio e non una zavorra, e ancora una volta i diritti degli utenti sono trattati come merce di scambio nel mercato della politica.

I soggetti più a rischio

Sono maggiormente in difficoltà le piattaforme la cui attività si basa sulla profilazione della propria utenza.