"Hatespeech? Faremo più controlli. Ma la vera sfida è l`educazione"
Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali
(di Francesco Lo Dico, "Il Dubbio", 17 gennaio 2018)

Migranti, donne, bambini. Il linguaggio dell'odio pervade social, siti e piattaforme ormai da anni, grazie alla complicità di nani e titani della rete, che troppo spesso hanno volto lo sguardo dall'altra parte, in nome della legge del clic che ha fatto strame di dignità, dati sensibili, e diritto alla privatezza. Una deriva segnalata e combattuta con forza sulle pagine di questo giornale, grazie all'iniziativa contro l'hate speech, lanciata a settembre dal Consiglio nazionale forense al G7 dell'avvocatura. Un segnale autorevole, che insieme a quelli lanciati dalla task force avviata dalla Commissione europea contro le fake news, e dal nostro governo con la legge contro il cyberbullismo in vigore da giugno, consentono al Garante della privacy, Antonello Soro, di segnalare un clima nuovo. *"La collaborazione avviata con i social network dall'Autorità per la protezione dei dati personali, ci ha permesso di fare progressi nel contrastare l'odio. E altri ne arriveranno, grazie all'accordo che abbiamo siglato sabato con la Polizia postale"*.

Presidente, che cosa prevede l'intesa?

E' necessario premettere che la legge Ferrara contro il cyberbullismo prevede per il Garante della privacy grandi responsabilità. Il provvedimento infatti assegna all'Autorità il ruolo principale sia nel prevenire la diffusione di link e video sgradevoli, sia nel rimuoverli entro 48 ore dalla segnalazione del giovane o della famiglia.

Non dev'essere semplice, dati precedenti come quello della piccola Carolina, la 14enne di Novara che si tolse la vita perché i suoi video intimi (fu stuprata dai compagni) circolavano su un sito giamaicano irreperibile.

Il dramma è che per una vittima di cyberbullismo 48 ore di tempo sono un'infinità: in due giorni i contenuti virali possono moltipllcarsi e creare contraccolpi drammatici. Ma allo stesso tempo 48 ore sono pochissime per chi deve intervenire. Ormai con i grandi social network c'è una collaborazione ben avviata, che permette interventi tempestivi. Quando invece si tratta di individuare i titolari di piccoli siti registrati all'estero e di imporre la rimozione di contenuti illeciti, bisogna avviare procedure di cooperazione con altri Stati che richiedono attività lunghe e complesse. A volte cancellare un video o un post che inneggiano all'odio o diffondono dettagli intimi, si rivela per il Garante una strada senza sbocco. Ed è proprio nell'ambito di questo quadro irto di insidie, che abbiamo stipulato il protocollo d'intesa con il capo della Polizia, Franco Gabrielli. Il Garante potrà contare su risorse e competenze di alto livello: quelle della Polizia postale.

Il comunicato che annuncia l'accordo fornisce dati preoccupanti. I casi di minori vittime di cyberbullismo sono in ascesa. Dalle 235 denunce del 2016 siamo arrivati alle 350 dell'anno scorso.

Si tratta di un'epidemia silenziosa. Al computo delle vicende note, bisogna infatti aggiungere la "cifra oscura" di molti casi che non fruiscono nei bilanci ufficiali. Troppo spesso nella vittima prevalgono la paura e la vergogna. Se intendiamo combattere a fondo il fenomeno, la chiave è realizzare un'alleanza tra scuole, famiglie ed agenzie educative. I genitori italiani, così come quelli di tutto il mondo, reagiscono spesso in modo scomposto. Urla e rabbia sono il modo peggiore di reagire, perché fanno chiudere i frgli a riccio.

In aiuto dei ragazzi potrebbe presto giungere anche il codice di regolamentazione dei social previsto dalla legge Ferrara. Sarà discusso a breve al ministero dell'Istruzione, insieme agli operatori della rete. Confida in un esito positivo?

E' di fondamentale importanza non affrontare le questioni sul tappeto con troppe lungaggini burocratiche. Servono agilità e concretezza per produrre misure efficaci. L'opera di responsabilizzazione dei giganti del web è già stata avviata, ma i loro doveri vanno ulteriormente precisati nero su bianco.

Intanto la task force della Commissione europea ha aperto ieri i lavori finalizzati a mettere un freno alle fake news. Si aspetta progressi anche su questo versante?

Il tema delle notizie false o fuorvianti dev'essere approcciato all'insegna della misura. Non si può correre il rischio di porre sotto controllo il sistema dell'informazione. Il confronto tra opinioni diverse, all'insegna del pluralismo, resta una risorsa fondamentale.

Zuckerberg ha per parte sua annunciato un nuovo algoritmo e l'assunzione di 10mila nuovi addetti che dovranno monitorare il linguaggio dell'odio. È la sconfitta dell'algoritmo, con il quale i big della rete pensavano di governare la rete grazie al pilota automatico?

La gestione di temi così delicati non può essere affidato esclusivamente a un algoritmo, è di tutta evidenza da tempo che la sensibilità umana è insostituibile. Affidare ai soli gestori il compito di prevenire il linguaggio dell'odio, rischia di accrescere i loro poteri già oggi smisurati. Sollecitare i social a intervenire, responsabilizzandoli, è utile. Ma il bilanciamento tra diritti fondamentali deve restare di competenza dell'autorità pubblica.

Facebook ha annunciato anche il riconoscimento facciale per contrastare gli account fasulli. E una specie di autodenuncia, in fase di test in Australia, che consente alla possibile vittima di inviare le proprie foto compromettenti alla piattaforma per prevenirne la diffusione. Che cosa ne pensa?

È necessario ricordare che i colossi della rete fanno già oggi ricorso a una raccolta massiva di dati personali, spesso anche biometrici, finalizzata a iniziative di profilazione commerciale. Nonostante si tratti di un meccanismo sempre più spesso accettato con inerzia dagli utenti, si tratta di un grande rischio per tutti. I dati personali sono infatti la maggiore risorsa dell'economia contemporanea, che li usa a fini commerciali. Dobbiamo essere consapevoli che ogni volta che acconsentiamo a cedere informazioni personali, stiamo cedendo un pezzo della nostra libertà.

Un fenomeno particolarmente preoccupante, quando riguarda i minori. Facebook sta per lanciare negli Usa Messenger Kids, il servizio di messaggistica per gli under 13. Nuovi rischi in vista?

Il nuovo regolamento europeo affida agli Stati il compito di individuare l'accesso ai social per i minori, entro un margine compreso tra i 13 e i 16 anni. In Italia, per varie ragioni, questa età potrebbe essere individuata intorno ai 14 anni. Ma ciò detto, è il dato reale la vera base di partenza. Uno studio autorevole dice che i bambini italiani tra i 5 e i 13 anni che navigano su internet sono il 44%, e di questi il 57% lo fa da solo, lontano dallo sguardo dei genitori. La vera svolta è nell'educazione civica dei piccoli. Ai bambini insegniamo ad attraversare la strada solo quando c'è il verde e fermarsi quando c'è il rosso, ma non abbiamo ancora insegnato loro come si vive nella società digitale.

Anche Google e Youtube preannunciano cambiamenti. Tutto ciò non succede certo per amore, ma per interesse. E così?

I colossi del web hanno ormai maturato la consapevolezza che contrastare l'odio, la discriminazione, il cyberbullismo e altri meccanismi perversi come la "revenge porn", os sia le vendette sessuali consumate dagli utenti tramite la pubblicazione di video intimi, non è una semplice questione di buona educazione. Le ingenti perdite pubblicitarie patite l'anno scorso, hanno inviato ai grandi player del settore un messaggio preciso: la cattiva reputazione può diventare la tomba dell'economia digitale.

Ha destato enorme clamore anche la vulnerabilità dei pc di tutto il mondo, dai quali possono essere rubati i dati personali. Possibile che delle falle nei processori non si fosse accorto nessuno?

E una domanda che andrebbe rivolta a chi negli ultimi dieci anni aveva il compito di individuare le falle che hanno messo a rischio i nostri computer. Il vero problema è che queste vulnerabilità possono essere sfruttate in misura maggiore di quanto non crediamo. L'Internet delle cose, le smart tv, le nuove auto, i dispositivi sanitari: tutto rischia di diventare hackerabile. Oggi l'umanità intera trascorre ampia parte della propria esistenza nella dimensione digitale. Sicurezza e protezione dei dati personali sono le frontiere più delicate e importanti di un mondo nuovo, ma pieno di incognite.