

AssetProtection. (Cyber) security e social accountability, due facce della stessa medaglia?

Parlare di (cyber) security e responsabilità sociale insieme potrebbe sembrare il maldestro tentativo di fare un'operazione matematica "mettendo insieme mele e pere". Ci hanno insegnato sin dalle elementari che non si fa. Però proseguendo con gli studi, ci hanno anche insegnato – si spera – a non fermarci alle apparenze, ad attivare un po' di sano senso critico. Ed è ciò di cui abbiamo più bisogno ora; è il momento di crescere collettivamente, di adattarci ad un contesto che il digitale ha reso profondamente differente rispetto al passato.

Ma se siamo dotati di senso critico, allora perché chi svolge la propria attività sotto il cappello della sostenibilità e si occupa di **CSR** non vuole saperne niente di privacy e security? Ed ancora, perché chi fa security ritiene che le vulnerabilità **Meltdown** e **Spectre** siano l'evento dell'anno, ma fa spallucce quando arriva la bacchettata dalla **Commissaria UE** alla Giustizia perché l'Italia, con la scusa delle elezioni, è indietro sul recepimento del **GDPR** a soli 100 giorni dalla data limite fissata? Come se poi le questioni politiche non avessero anche a che fare con i sistemi IT. Insomma tutti al riparo, ciascuno nel proprio orticello (professionale e linguistico).



Allora ripartiamo dall'inizio. Proviamo ad inquadrare la situazione con un sillogismo aristotelico. Affermazione A: Informazioni e strumenti digitali sono pericolosi, se poco o mal governati. Affermazione B: Una porzione significativa della popolazione mondiale (più di quattro miliardi di persone

connesse) è a stretto contatto con informazioni e strumenti digitali. Conclusione: Una porzione significativa della popolazione mondiale è in pericolo se governa poco o male informazioni e strumenti digitali. Corretto? E non stiamo parlando di pericolo economico. Stiamo parlando di pericoli non quantificabili, come la violazione dei diritti dell'uomo. Ad esempio, nella Carta dei Diritti Fondamentali dell'Unione Europea si parla di diritto alla protezione dei dati di carattere personale (ex. Art. 8).

Per comprendere quanto sia concreta l'urgenza di includere la (cyber) security nell'ambito della responsabilità sociale basti riflettere sul modo in cui si sta rapidamente modificando il settore industriale. Uomini e macchine "intelligenti", ma pur sempre governate da software e connesse a reti violabili, sono a contatto strettissimo. Paradossalmente, un Responsabile Sicurezza Prevenzione e Protezione dovrebbe essere un esperto in informatica per comprendere se le misure di governo sui sistemi IT siano idonee a garantire l'incolumità delle persone; ma sappiamo bene che questa non è la realtà.

Infine qualche ulteriore problema lo genera anche un altro grave errore concettuale generalizzato: classificare linguisticamente le persone a seconda degli ambienti nei quali svolgono le loro attività ed interagiscono con altre persone. Una persona al lavoro è una risorsa. Una persona a casa è un marito o una mamma. Una persona che prende un mezzo di trasporto è un passeggero, una persona che acquista è un cliente e così via scorrendo. Non si può più credere di applicare alcune specializzazioni professionali a singole classificazioni nominali. Con questo non dico di risolvere il problema con una disastrosa "tuttologia", alla quale in ogni caso i media tentano di abituarci, bensì con un atteggiamento orientato alla convergenza delle competenze.

Anche l'organizzazione Global Reporting, una vera e propria punta di diamante nella definizione dei criteri per la messa a

punto dei bilanci di sostenibilità, sembra ancora non aver bene messo a fuoco la questione. Il tentativo di portare la privacy nella rendicontazione di sostenibilità c'è (si veda il modulo GRI 418 – Privacy del cliente), ma la struttura è ancora molto spoglia, troppo debole. Invece il **SAI** (Social Accountability International), che si occupa di promuovere i diritti dei lavoratori in tutto il mondo, ha deciso di non considerare neanche minimamente la questione nell'ultima versione dello standard SA8000 del 2014.

Ma almeno i professionisti che si occupano della materia ne comincino a discutere. Che trasmettano l'urgenza di colmare tutte le lacune che emergono in un sistema che non tiene conto delle innumerevoli implicazioni connesse allo sviluppo tecnologico degli ultimi vent'anni. Che si attivino mentalmente, con uno spirito rinnovato. Per aiutare la società a progredire, a crescere, attraverso adeguati processi di conoscenza e di sostenibilità.

AssetProtection. (Cyber) security e social accountability, due facce della stessa medaglia?