GDPR. È ora di *mappare* le **vulnerabilità**

ALGORITMI DI MACHINE LEARNING E DI RICONOSCIMENTO SEMANTICO POSSONO AIUTARE LE BANCHE A SCOVARE I DATI SOGGETTI ALLE NORMATIVE PER LA PRIVACY DISTRIBUITI NEI LORO SISTEMI INFORMATIVI. PERCHÉ NELL'ERA DEI BIG DATA LE INFORMAZIONI CRESCONO ESPONENZIALMENTE, E LA RICERCA DELLE VULNERABILITÀ HA BISOGNO DELLE NUOVE TECNOLOGIE

Molte aziende non si sono ancora attrezzate per il GDPR, o quantomeno non in maniera soddisfacente, e la mancanza di una soluzione univoca per essere compliant alla normativa rende questo adeguamento ancora più complicato. A raccontarlo è Rino Adamo, Amministratore Delegato di RES e Presidente di RES Academy, che sottolinea come «in questo processo di compliance sia importante per le aziende procedere con una valutazione iniziale del contesto in cui si muovono, così da creare una mappa dei potenziali documenti e dati presenti nel proprio sistema informativo che contengono elementi impattati dalla problematica del GDPR».



Rino Adamo, Amministratore Delegato di RES e Presidente di RES Academy

Alla ricerca del dato sensibile...

Per scandagliare tutti gli elementi legati ai dati soggetti a privacy, RES ha messo a punto due tecnologie che lavorano in maniera sinergica «e riunite nella GDPR Discovery Suite – racconta Adamo. Un tool, GDPR Document Analyzer, è orientato all'analisi dei documenti, mentre l'altro, il Data Meaning Discovery, è stato creato per la ricerca di dati sensibili all'interno dei database. Lo scopo è individuare negli spazi di storage indicati dalle aziende (tra cui server, pc, database relazionali o file) dati strutturati e non, che contengano informazioni legate alla privacy e quindi soggette ai vincoli normativi del GDPR».

...con algoritmi di machine learning

Un lavoro non semplice, vista la mole di dati che continua a crescere in modo esponenziale, andando a prendere posto in milioni di documenti o di archivi. «Al di là quindi delle azioni, organizzative e tecnologiche, che possono essere messe in campo, bisogna capire dove sono queste informazioni sensibili che devono essere protette e soprattutto rese note – spiega Adamo. Alla base delle nostre due soluzioni sono quindi presenti degli algoritmi di machine learning e di riconoscimento semantico all'interno dei testi, creati all'interno del laboratorio RIDS (RES Institute for Data Science) in collaborazione con i ricercatori dell'Università di Pavia».

Un processo automatizzato

Il risultato è una mappa capace di identificare le probabilità che un determinato documento, tabella o file, contenga informazioni soggette a privacy. «Gli utilizzatori avranno a disposizione le informazioni da consultare o da integrare con propri sistemi e/o soluzioni – continua Adamo. Inoltre, il sistema opera in maniera totalmente automatica: è infatti un processo robotizzato molto efficiente, che riesce a censire un numero di informazioni elevatissimo in tempi molto rapidi».

Dall'assessment all'azione

Le potenziali criticità vengono quindi allo scoperto. «E in questo modo, si può procedere con un assessment iniziale delle vulnerabilità presenti, anche dal punto di vista di informazioni che sono soggette a privacy ma ancora non adeguatamente protette o conosciute, per individuarle e passare quindi all'azione. Ma RES può fare molto più di questo per i propri clienti – conclude Adamo – potendo mettere in campo, oltre alla tecnologia e attraverso la proprio rete di partner, competenze organizzative e strumenti a supporto dei processi di governance delle problematiche legate al GDPR, sia per quanto riguarda la Compliance, la Data protection & Security e le funzioni di DPO».

G.C.