Information Security, Data Protection e Privacy

Information Security, Data Protection e **Privacy**: questi tre termini vengono spesso usati come sinonimi, ignorando le caratteristiche che ne sostanziano le differenze. È così che, soprattutto in contesti colloquiali, si parla indistintamente di *Information Security, Cybersecurity* o anche Sicurezza, Privacy e protezione dei dati. Allo stesso modo ci si riferisce al "Garante Privacy" o alla "normativa sulla privacy", intendendo invece il Garante per la protezione dei dati personali; la normativa sulla protezione dei dati, d'altronde, viene indicata anche come normativa sulla "sicurezza".

Mantenere una chiara distinzione terminologica non è un puro esercizio accademico o una questione di stile: i concetti di *Information Security, Data Protection* e di privacy sono sorretti da sostanziali distinzioni concettuali con implicazioni pratiche, nelle attività operative di ogni azienda e organizzazione, che trovano fondamento nella storia dell'uomo, del diritto e dell'evoluzione tecnologica e normativa.

Con il termine ***Information Security,*** non si intende solamente la protezione delle informazioni da accessi non autorizzati. Chiamiamo "informazioni" tutti gli insiemi di dati che vengono elaborati, strutturati e presentati in relazione ad uno specifico contesto, all'interno del quale assumo un significato altrimenti non rinvenibile. I dati, al contrario, rappresentano un fatto grezzo, non organizzato, che deve essere elaborato per renderlo significativo. I dati devono quindi essere sempre interpretati, da un essere umano o da una macchina, per derivarne il significato. I dati, decontestualizzati, non hanno un proprio significato intrinseco. I dati, possiamo dire, hanno bisogno di essere

raffinati, come il petrolio, prima di acquisire valore spendibile ed essere utilizzati.

ISO[1] definisce nella norma internazionale ISO/IEC 27000:2018[2] il termine *Information Security* come "*preservation of confidentiality, integrity and availability of information*"[3]. L'*Information Security*, si occupa dunque della protezione della riservatezza, integrità e disponibilità di qualsiasi tipologia di informazione, all'interno di qualsiasi organizzazione e si concretizza nella pratica di prevenire l'accesso, l'uso, la divulgazione, l'interruzione, la modifica, l'ispezione, la registrazione o la distruzione non autorizzata delle informazioni.

Il termine ***Data Protection*** non deve far pensare, in contrapposizione a quanto detto in precedenza, alla protezione dei dati. Il significato di *Data Protection* diventa chiaro, richiamando le differenze con il termine Privacy. A questo fine è bene ricordare come il termine **Privacy** abbia origine nord-americana. Gli studiosi fanno risalire l'origine del termine Privacy, al 1890 quando Samuel D. Warren e Louis D. Brandeis, due giuristi di Boston, pubblicarono sull'Harvard Law Review[4] un articolo dal titolo "*The right to Privacy*". In questa pubblicazione la privacy è vista come la necessità di salvaguardia della sfera più "intima" dell'essere umano: la necessità di non vedere invaso il proprio spazio abitativo, le relazioni familiari e tutto ciò che si svolge al suo interno. Questa necessità non è certo diversa e distante dai bisogni fondamentali dell'uomo teorizzati da Abraham Maslow nel 1954, il quale ha evidenziato come i bisogni di sicurezza, appartenenza, stima e autorealizzazione, ciascuno con le proprie specificità e ognuno declinabile in ulteriori fabbisogni specifici, siano alla base dell'agire umano: fin dalle sue origini.

Il bisogno "primordiale" della salvaguardia della privacy è, quindi, alla base del pragmatismo umano.

La *Data Protection*, più strettamente legata al contesto culturale e storico europeo, si è significativamente sviluppata anche in conseguenza delle guerre che hanno interessato (non solo) il nostro continente nel corso del secolo scorso, quando i dati relativi a persone fisiche potevano essere usati – e venivano usati – per controllare e discriminare le persone. È stato così con le attività condotte su larga scala da vari governi in differenti nazioni, a proposito di anziani, ammalati, omosessuali, partiti politici e professioni religiose. La cultura della *Data Protection* nasce quindi dalla necessità di proteggere le persone fisiche, prima ancora del dato o dell'informazione in quanto tale, dal controllo invasivo operato da governi e nazioni e dall'utilizzo automatizzato e indiscriminato dei dati personali.

Dagli anni '80 del secolo scorso si sono susseguite diverse attività normative a livello europeo culminate nel Regolamento (UE) 2016/679, noto come **GDPR** (o RGPD in italiano), il cui obiettivo è proprio la protezione delle persone fisiche per quanto attiene al trattamento dei loro dati personali, dal cui scorretto uso possono derivare gravi lesioni delle libertà e dei diritti degli individui. Il diritto alla protezione dei dati personali, è bene ricordare, *"non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità"*[5]. Inoltre, l'articolo 12 della Dichiarazione universale dei diritti umani, recita: *"Nessun individuo potra` essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, ne´ a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni".* È curioso osservare quanto spesso anche il GDPR, e la sua implementazione, venga con troppa leggerezza criticato, accusando costrizioni e limitazioni di presunte libertà prive di qualsiasi fondamento.

La *Data Protection* si occupa, quindi, della protezione delle persone fisiche; la privacy è più legata alla sfera "intima" dell'essere umano; l'*information security* si occupa di qualsiasi tipo di informazione. Anche per questo motivo, ad esempio, **non tutti gli incidenti di sicurezza delle informazioni rappresentano anche un *data breach***, mentre quest'ultimo implica certamente una violazione nella sicurezza delle informazioni.

Possiamo quindi pensare al dominio di competenza di *Information Security, Data protection* e Privacy come tre cerchi concentrici, con la prospettiva più ampia secondo la quale l'*Information Security* ingloba la *Data protection* e la privacy. Queste ultime due, pur condividendo "il dato", hanno prospettive diverse: la prima si occupa della protezione delle persone fisiche, mentre la seconda è più concentrata sulla protezione di informazioni di persone fisiche.

È dunque chiaro come mai risulti scorretto e approssimativo l'indifferente utilizzo dei termini *Information Security, Data Protection* e Privacy.

Note

[1] International Organization for Standardization

[2] Information technology – Security techniques – Information security management systems – Overview and vocabulary

[3] ISO/IEC 27000:2018(en), § 3.28: information security: preservation of confidentiality (3.10), integrity (3.36) and availability (3.7) of information.
Note 1 to entry: In addition, other properties, such as authenticity (3.6), accountability, non-repudiation (3.48), and reliability (3.55) can also be involved

[4] Warren, Samuel D., and Brandeis, Louis D., *The Right to Privacy*, Harvard Law Review, vol. 4, no. 5, 1890, pp. 193–220. JSTOR, www.jstor.org/stable/1321160.

[5] Regolamento (UE) 2016/679, Considerando 4.

Articolo a cura di **Luciano Quartarone**

https://www.ictsecuritymagazine.com/articoli/information-security-data-protection-e-privacy/