# Niente proroghe sul GDPR, il 25 maggio 2018 non si tocca

Il **GDPR non ammette proroghe**, ripensamenti o altre manipolazioni 'territoriali' a livello di entrata in vigore. Ogni stato membro europeo dovrà attenersi strettamente al dettato del regolamento che, in quanto tale, già ha definito le linee guida di intervento anche a livello sanzionatorio. Si ricordi, infatti, che per un illecito trattamento dei dati ci sarà una sanzione amministrativa e pecuniaria fino a 20 milioni di euro e fino al 4% del fatturato mondiale annuo dell'esercizio precedente se superiore ai 20 milioni di euro.

**Francesco Maria Pizzetti, ordinario di diritto costituzionale (Università degli studi di Torino) e presidente dell'Autorità Garante per la privacy tra il 2005 e il 2012,** parla chiaro, intervenuto a un recente evento svoltosi presso la sede del data center di **T.net**. *"Nessuno Stato potrà adottare per sé una normativa differente da quella dettata nel regolamento* – tuona Pizzetti – *perché il regolamento europeo, in quanto tale, è già entrato in vigore e non è una direttiva*".

Un problema che, in un certo senso, impatterà sul GDPR è quello legato a due articoli contenuti nella legge europea numero 167 del 2017, già uscita in Gazzetta Ufficiale, con i quali, di fatto, **si autorizzerebbero, senza bisogno del consenso, le multinazionali a trattare i nostri dati, presumibilmente a partire da quelli sanitari.** Su questo fronte, *Silicon* ha interpellato Pizzetti, che afferma: "*L'anomalia dell'articolo 28 che consente un riutilizzo di dati sensibili per generiche finalità scientifiche subordinate solo ad autorizzazione del garante, per come è scritta la norma non si capisce se questa debba essere basata sulla verifica della minimizzazione dei dati o sull'anonimizzazione. Se fosse basata su questo secondo punto, come molti ritengono, allora il garante diventerebbe un soggetto che si limita a verificare che i dati siano effettivamente anonimizzati, il che va contro il vero ruolo del garante che è quello di autorità di controllo. Allo stesso tempo* – continua – *la norma introduce l'articolo 110 bis al codice di protezione dei dati personali e quindi sembra far riferimento anche e specificatamente ai dati relativi alla salute che, che sono quelli regolati, il cui utilizzo è regolato con modalità specifiche e diverse dall'articolo 110 del codice. Inoltre* – conclude – *l'articolo 28, vietando ogni riutilizzo di dati genetici, chiude le porte in modo tranchant alla possibilità di istituire gruppi di ricerca in ambito genetico che, sulla base di vincoli e norme contenute nel GDPR, e anche nella stessa autorizzazione generale del garante, possono comportare la necessità di scambiare questi dati tra gruppi di ricerca che perseguano la stessa finalità".*

Ma si pensi ancora all'**avvento dell'intelligenza artificiale o del machine learning**, la comunicazione tra macchine e lo scambio di dati, dovrà trovare chiarezza nel GDPR. "*Servono le specifiche che il garante europeo darà e nel prossimo futuro, quando arriveranno novità come machine learning che portano all'utilizzo di una mole di dati non indifferente, si dovrà regolamentare l'uso di questi particolari dati tecnologici*", chiude Pizzetti.

Un tracciato chiaro che è stato scolpito nella testa dei presenti all'evento "GDPR 2018 – Nuova normativa e Infrastruttura IT: aspetti critici e opportunità per il business delle imprese" organizzato presso la sede del MIX (Milan Internet Exchange) a Milano, luogo nel quale è presente anche il data center di T.net, infrastruttura e ingegneria It per l'innovazione, che ha affrontato questi temi, intrecciati con temi altrettanto 'moderni' a cura di **Francesco Mazzola, ceo di T.net Italia**. Le

parole del docente ed ex presidente del Garante hanno messo fine a un concetto, forse fin troppo italiano, quello della proroga di una normativa che è già entrata in vigore e dal 25 maggio 2018, chi sarà trovato impreparato o non compatibile con la normativa europea, sarà sanzionato pesantemente. Insomma, dal Codice sulla privacy al GDPR il passo è significativo. E non si scherza con la normativa europa che di fatto falcerà ogni normativa italiana in merito alla protezione dei dati.

Mazzola interviene facendo leva sul fatto che oggi molto si rifà sui temi quali cloud, IoT, che tante volte abbiamo sottolineato, muoveranno non pochi dati e quindi ora più che mai ci si deve interrogare sulla sicurezza delle reti e sulla gestione degli stessi dati. Mazzola non si tira indietro parlando di certificazioni e di interventi preso i clienti per realizzare materialmente l'infrastruttura necessaria e, quando si parla di reti, va chiarito chi si occupi di queste, chi gestirà l'infrastruttura.

A ricordarci il fatidico 25 maggio 2018, **Chiara Agostini, avvocato di R&P Legal, Studio Legale di Milano,** intervenuta anch'essa all'evento ha affermato che la privacy ha una doppia faccia: da un lato le misure di sicurezza organizzative che riguardino i contratti che regolano i rapporti tra i vari soggetti coinvolti, ma per avere sicurezza delle banche dati è necessario che i contratti e le policy aziendali vivano di pari passo con software e infrastrutture sicure. **La normativa sul GDPR è già entrata in vigore ma sarà vincolante,** appunto dal 25 maggio del prossimo anno e "*sarà direttamente applicabile a tutti gli stati membri. Infatti* – spiega Agostini – *stiamo parlando di un regolamento e non di una direttiva. Ma cosa ne sarà del codice privacy e dei provvedimenti che il garante ha emesso negli ultimi 15 anni? Non abbiamo ancora una risposta formale* – spiega l'avvocato – *l'approccio del Garante è ancora prudente dato che non è ancora stata formalizzata chi sarà l'autorità di controllo competente. Quello che oggi si sa* – continua Agostini – *è che il* ***17 ottobre 2017 è stato approvato un testo di delega al Governo per il recepimento della normativa anche sul GDPR*** *quindi, questo significa che entro maggio il governo si esporrà per affermare quali parti della normativa sulla privacy attualmente in vigore resteranno e quali no".*

Insomma, con il recepimento di questo regolamento, si apriranno parecchi scenari. L'avvocato ha messo in luce come le aziende e non solo dovranno sempre farsi domande sulla natura dei dati da trattare e chiedersi se tutti quei dati serviranno allo scopo. Agostini fa proprio un esempio a riguardo. *"Si pensi a un'attività di direct marketing. Le aziende dovrebbero valutare che i dati necessari per questa attività siano solo nome, cognome e mail mentre la professione non sia un requisito necessario, a meno che non si debba fare anche profilazione, stessa cosa per l'età"*, conclude.