



## **Regolamento UE. "Illeciti, non soltanto sanzioni. Le reazioni saranno diverse. In un approccio graduale"**

Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali

(di Antonio Ciccina Messina, "Italia Oggi", 21 maggio 2018)

Non solo sanzioni amministrative nel Regolamento Ue sulla privacy. Le reazioni possibili dell'ordinamento alle violazioni sui dati sono diverse e dovranno seguire un approccio gradualistico. A sottolinearlo è Antonello Soro, presidente dell'Autorità garante italiana, che, rispondendo a ItaliaOggi Sette a pochi giorni dal debutto del "Gdpr" (il regolamento 2016/679 sulla protezione di dati), detta le priorità per aziende ed enti alle prese con le nuove sfide poste dalla normativa europea. In cima all'agenda, la formazione del personale e la sicurezza informatica.

### **Presidente Soro, il Regolamento europeo nasce in un clima di incertezza e di ansia per le imprese. Quali sono gli adempimenti ai quali si consiglia di dare priorità?**

*Il Regolamento è in vigore già da due anni e sulle sue innovazioni il Garante ha promosso un'attività formativa ad amplissimo spettro, proprio al fine di promuoverne la conoscenza da parte di imprese e amministrazioni. Naturalmente, il ritardo nell'approvazione del decreto legislativo di adeguamento può ingenerare incertezza rispetto alle modifiche da apportare alla propria attività aziendale, inducendo a ripensare assetti o modalità organizzative, consolidati a volte più per inerzia che per reale utilità. Ma l'adeguamento al Regolamento si rivelerà una straordinaria opportunità, per consentire ad aziende e amministrazioni di stare al passo con l'innovazione e le nuove sfide di un'economia fondata sui dati, nonché per investire sulla protezione dati quale risorsa reputazionale essenziale e fattore di vantaggio competitivo. Adempimenti fondamentali, in questo senso, sono un'adeguata formazione del personale, modulata naturalmente sulla base delle specifiche mansioni di ciascuno, una puntuale ricognizione delle misure di sicurezza, tecniche e organizzative, che dovranno essere adeguate alle caratteristiche del trattamento, una complessiva revisione delle proprie informative per adeguarle all'impostazione più sostanzialistica del Regolamento, nonché la predisposizione delle procedure necessario ad effettuare, ove ne ricorrano i presupposti, la notifica dei data breach. Per rendere più agevole il processo di adeguamento al Regolamento, è poi opportuno, per le imprese che vi siano tenute ma anche, auspicabilmente, per le altre, nominare il Dpo, che possa indirizzare le scelte aziendali nella direzione della compliance. Coloro i quali vi siano tenuti, dovranno poi provvedere ad adempimenti essenziali quali la valutazione d'impatto privacy (e, nel caso di persistenza di rischi, la consultazione preventiva del Garante) o il registro delle attività di trattamento.*

### **Gli enti pubblici sono generalmente molto indietro nell'applicazione del regolamento Ue. Sono in programma linee guida o interventi simili da parte del Garante e su quali argomenti?**

*Non abbiamo elementi per ritenere che gli enti pubblici siano indietro nell'applicazione del Regolamento; per parte nostra abbiamo organizzato, in varie regioni italiane, numerosi incontri formativi con i rappresentanti delle amministrazioni, proprio al fine di accompagnarle nell'attività di adeguamento al nuovo quadro giuridico europeo. Abbiamo pubblicato specifiche linee guida e faq, nonché un cospicuo materiale informativo sul Regolamento. A seguito dell'approvazione del decreto legislativo di adeguamento, che introduce norme di raccordo con l'ordinamento interno e della prima attuazione della disciplina, valuteremo gli interventi da compiere in ragione delle specifiche esigenze che si dovessero presentare.*

### **Il Garante predisporrà regole di graduazione delle sanzioni amministrative per distinguere violazioni formali da quelle più gravi?**

*Il Regolamento delinea un sistema sanzionatorio alquanto articolato. Anzitutto, configura la sanzione amministrativa come una delle possibili "reazioni" (non certo l'unica) dell'ordinamento all'illecito, da applicarsi secondo un approccio gradualistico, congiuntamente o alternativamente alle misure inibitorie e prescrittive. La scelta in ordine all'an della sanzione deve fondarsi sugli stessi parametri indicati dal Regolamento per la commisurazione infraeditale della sanzione pecuniaria (gravità dell'illecito desunta anche dal danno che ne sia derivato, elemento soggettivo, eventuale ravvedimento operoso o, al contrario, recidiva, categorie di dati interessate dalla violazione, adesione a codici di condotta o sistemi di certificazione, cooperazione con l'autorità di controllo ecc.). La norma fornisce già, dunque, elementi sufficienti per distinguere gli illeciti in ragione della loro gravità, ai fini della scelta tanto sull'an quanto sul quantum della sanzione.*

### **Il settore Pmi è sempre in attesa di semplificazioni. Nelle more devono eseguire tutti gli adempimenti che il regolamento Ue prescrive senza distinzioni. Non sarebbe opportuno indicare in concreto e al più presto quali sono le disposizioni ufficiali per piccole e medie imprese?**

*Il Regolamento già di per sé modula gli adempimenti previsti in capo al titolare in ragione, tra l'altro, della dimensione dell'impresa e, quindi, dell'ambito di incidenza del trattamento, come abbiamo chiarito anche in diversi incontri con esponenti del mondo imprenditoriale e, in particolare, associazioni di categoria. La disciplina europea, che mira a rafforzare "il clima di fiducia che consentirà lo sviluppo dell'economia digitale" nel mercato interno, coniuga la protezione dati con istanze di semplificazione, che il decreto di adeguamento peraltro valorizza, prevedendo che rispetto alle micro, piccole e medie imprese il Garante possa promuovere modalità semplificate di adempimento agli obblighi del titolare.*