GDPR, TANTO RUMORE PER NULLA

di GIACOMO CORVI

NONOSTANTE LE ASPETTATIVE, L'ADEGUAMENTO AL NUOVO REGOLAMENTO È STATO VISSUTO DALLE AZIENDE COME UN ATTO BUROCRATICO: SOLUZIONI LOW COST E POCHI INTERVENTI DI AMPIO RESPIRO. INTANTO, IL CYBER RISK SI CONFERMA UNA DELLE MINACCE PRINCIPALI AL NOSTRO PATRIMONIO INFORMATIVO

Più di un anno fa entrava in vigore il *Gdpr*. Le aspettative di istituzioni e autorità di vigilanza, verso questa innovativa disciplina per il trattamento dei dati personali, erano alte. La vigilia dell'entrata in vigore, funestata da una serie di attacchi informatici su larga scala che aveva fatto ben comprendere la portata della minaccia cibernetica, era stata vissuta in un clima quasi millenaristico: fiumi di inchiostro sono stati riversati su articoli, analisi, rapporti e possibili previsioni di come sarebbe cambiato il mondo dopo l'attivazione del regolamento europeo. Poi, alla fine, il 25 maggio 2018 è arrivato. E poco o nulla è cambiato.

"L'adeguamento alla disciplina è stato per le aziende un atto quasi burocratico, da sbrigare velocemente e al minor costo possibile", ha allargato le braccia **Nicola Bernardi**, presidente di **Federprivacy**. "Molte imprese – ha aggiunto – si sono orientate verso soluzioni low cost, cercando una scorciatoia che consentisse di raggiungere il minimo sindacale e convincersi di essersi messi in regola". Un modello virtuoso di gestione dei dati personali e del rischio informatico, che poi è il vero obiettivo del Gdpr, pare ancora di là da venire. Eccezion fatta per le grandi aziende, la situazione in Italia resta assai precaria. "La cognizione del rischio fra le microimprese è prossima allo zero, la stragrande maggioranza delle aziende di piccole e medie dimensioni ha fatto pochissimo", ha proseguito Bernardi.

UNA LEGGE NON BASTA

Secondo alcuni, si comincerà a vedere qualcosa quando arriveranno le prime sanzioni. Già, peccato però che, come ha osservato Bernardi, "le prime sanzioni sono già arrivate, anche piuttosto pesanti. Lo **European Data Protection Board** sta pubblicando i vari provvedimenti, ma non sta cambiando nulla".

La realtà è che forse leggi e sanzioni non bastano. Innanzitutto perché, come ha osservato **Umberto Rapetto**, ex generale della **Guardia di Finanza** e cyber security advisor, "l'iter legislativo ha una durata che collide con la velocità con cui evolvono le minacce informatiche". E poi perché le sanzioni non sembrano fare così paura. "Nessuno si è spaventato – ha ricordato Rapetto – quando la disciplina del 1996 parlava di anni di reclusione per chi non adottava misure di sicurezza adeguate". In questo contesto, fra beneficio della norma e rischio di eventuali sanzioni, il crinale resta sottile. E un'azienda non conforme alla normativa, in caso di attacco informatico, può ritrovarsi allo stesso tempo vittima e imputato. "La disciplina sulla riservatezza dei dati prevede sanzioni per chi non ha disposto misure di sicurezza: avete idea di qualcuno che va ad autodenunciarsi?", ha chiesto Rapetto.

Da sinistra: ***Umberto Rapetto****, ex generale della Guardia di Finanza e cyber security advisor;* ***Maria Rosa Alaggio****, direttore di Insurance Review; e* ***Nicola Bernardi****, presidente di Federprivacy*

VIRUS ED ERRORI IN BUONA FEDE

Poco, insomma, ha potuto la paura delle sanzioni. Ancor meno, se possibile, hanno potuto le sempre più frequenti notizie di attacchi o incidenti informatici. "A Baltimora, nel Maryland – ha portato l'esempio Rapetto – hanno passato quasi tre settimane avvolti in una sorta di oscurità digitale: il black out ha portato alla paralisi di tutti i servizi, con pesanti ripercussioni su qualsiasi attività di tipo amministrativo". Alla base di tutto c'era un *ransomare*, un software malevolo che infetta i dispositivi, cripta i dati e chiede il pagamento di un riscatto per ripristinare le funzionalità del sistema. "È la minaccia più angosciante – ha osservato Rapetto – perché può colpire chiunque: da Baltimora a casa nostra".

A volte, tuttavia, il rischio può arrivare anche da una semplice disattenzione. "Un paio di mesi fa – ha affermato Bernardi – siamo stati contattati da una grande azienda con 1.400 dipendenti che aveva riscontrato un problema nel recapito delle e-mail con le buste paga: al posto dei dati del singolo destinatario, il file allegato conteneva le retribuzioni di tutti i suoi colleghi". Tutto ciò, ha proseguito Bernardi, era dovuto a un errore in buona fede del responsabile dell'invio. Però le conseguenze, in termini di privacy, si sono fatte sentire.

CERCASI DATA PROTECTION OFFICER

Basterebbero questi due esempi per comprendere la gravità della minaccia. Eppure, parafrasando Ennio Flaiano, la situazione della sicurezza informatica in Italia "è grave ma non seria". Lo si capisce vedendo come le imprese hanno risposto all'obbligo previsto dal Gdpr di istituire la figura del *data protection officer*. Anche in questo caso, ha affermato Bernardi, si è spesso optato per "soluzioni low cost, con personale che talvolta non presenta neppure le competenze necessarie per assumere il ruolo". Nato come figura indipendente e libero da ogni conflitto di interessi, il data protection officer si trova nei fatti "in una posizione di assoluta debolezza, senza neppure un budget di cui disporre: il regolamento prevede che sia prontamente coinvolto in caso di necessità, ma spesso e volentieri – ha aggiunto Bernardi – è l'ultimo a essere interpellato".

Sulla stessa linea anche Rapetto, il quale ha puntato il dito contro "i data protection officer improvvisati, quelli che nella loro vita hanno maneggiato al massimo un *Game Boy* e si sono svegliati una mattina esperti di cyber security". Rivolgersi a un incompetente, magari solo perché pratica tariffe convenienti, "è l'azione più criminale e suicida che possa commettere un imprenditore", ha osservato Rapetto.

ANONYMOUS NON SCHERZA

La scarsa attenzione che le imprese hanno riservato al Gdpr è sintomatica di una percezione del rischio che resta ancora poco diffusa. E, in questo caso, a poco possono servire le leggi. "Nessuna normativa – ha commentato Rapetto – potrà mai imporci di stare attenti, di essere accorti e non mettere a repentaglio il nostro patrimonio informativo". Quello che manca, ha aggiunto, è uno scatto culturale che ci spinga a "metterci davanti a uno specchio per confrontarci sinceramente con noi stessi su quello che abbiamo fatto per tutelare la nostra privacy". Altrimenti c'è anche il rischio che la realtà superi la nostra mancanza di volontà. "Hacker come **Anonymous** non si accontentano di finire sui giornali: arriverà il giorno in cui smetteranno di scherzare", ha affermato Rapetto. "Quel giorno, se non avremmo preso tutte le contromisure – ha chiosato – probabilmente non saremmo neppure in grado di accendere il computer su cui vogliamo scrivere l'articolo che racconti questa storia".