«Sicurezza da adeguare»

INFORMATICA / L'anno prossimo entra in vigore la nuova legge federale sulla protezione dei dati che rafforzerà i diritti dei cittadini
Le aziende e le amministrazioni pubbliche, però, dovranno adattarsi e meglio proteggersi in caso di attacchi informatici

Paolo Gianinazzi

Entro la fine del 2022 in Svizzera entrerà in vigore la revisione totale della Legge federale sulla protezione dei dati (LPD). Una legge complessa, che avrà un impatto su tutti noi. Il suo obiettivo principale, in sintesi, è proteggere al meglio i dati personali e sensibili dei cittadini. Di conseguenza, anche tutti coloro che trattano i nostri dati (le aziende e le pubbliche amministrazioni in primis) dovranno adattarsi alla nuova normativa. Un processo non semplice e che, dal punto di vista informatico richiederà un vero e proprio cambio di passo nel nostro Paese.

Per prepararsi al meglio gli adetti ai lavori al cambiamento, nel corso dell'anno il Gruppo di lavoro strategico "Cyber sicuro" si è adoperato per informare specifici settori riguardo alle novità che questa nuova legge porta con sé. E ieri, è stata organizzata a Lugano una conferenza aperta a tutti dedicata proprio alla nuova legge. Ma, concretamente, cosa cambierà nel momento in cui il testo e la relativa ordinanza entreranno in vigore? «Una delle principali novità riguarda il fatto che le aziende, così come le pubbliche amministrazioni, dovranno fare tutto ciò che è plausibile fare per prepararsi a un eventuale incidente informatico», ci spiega Alessandro Trivilini, membro di "Cyber Sicuro" e responsabile del Servizio informatica forense della SUPSI. In buona sostanza, nel caso di un attacco informatico, le imprese e le pubbliche amministrazioni dovranno poter dimostrare di aver fatto tutto il possibile per evitarlo o per mitigarne le conseguenze. Ciò comporta rispettare gli standard minimi di sicurezza chiesti dalla Confederazione e avere delle procedure precise. «Non dovranno tutti diventare delle enormi centrali informatiche», precisa Trivilini, «tuttavia sarà necessario adottare quei comportamenti di responsabilità e consapevolezza che permettano di dimostrare a chi avrà il compito di capire cosa è successo durante l'attacco informatico quali erano le responsabilità e come si è agito per affrontarlo». Tutti, dunque, «dovranno avere un piano di risposta in caso di un attacco». E da questo punto di vista, ci spiega Trivilini, «oggi in Ticino andiamo a due velocità: le aziende che trattano dati personali con Paesi dell'Unione europea sono già sensibili sul tema, perché il relativo regolamento europea (il "famoso" GDPR) già lo prevede sin dal 2018. Le altre aziende, invece, sono rimaste un po' più indietro e dovranno adeguarsi».

In Ticino sul fronte della sicurezza informatica resta ancora molto lavoro da fare. © CDT/ZOCCHETTI

Anche sul fronte delle pubbliche amministrazioni resta ancora diverso lavoro da fare. Come ci spiega il co-direttore del Centro di Calcolo Elettronico SA Giorgio Rastrelli, che da anni lavora fianco a fianco agli Enti locali, «non siamo messi benissimo». Anche se, va detto, «non si tratta di un problema ticinese o dei Comuni. È un problema generalizzato di mancanza di consapevolezza, sia nel pubblico sia nel privato». Tuttavia, aggiunge, «qualcosa sta pian piano cambiando e dal nostro osservatorio possiamo dire che circa il 20% dei Comuni si è mosso per adattarsi». E oltre alla mancanza di consapevolezza, la criticità più grossa, spiega Rastrelli, «è legata al fatto che i Comuni più piccoli non hanno, per ovvi motivi, la capacità tecnologica per poter dare una risposta alle problematiche che stanno sorgendo. L'informatica è diventata un mondo molto complesso e difficilmente un Comune di 3 mila abitanti può stare al passo da solo, diventando però vulnerabile agli attacchi». E quindi, il consiglio ai Comuni è quello di «prendere consapevolezza del problema e rivolgersi a fornitori esterni e affidabili».

Ma pure sul fronte delle aziende private, spiega l'avvocato Rocco Talleri, «c'è ancora molto da fare». E la parola chiave, anche in questo contesto, è consapevolezza: «Le aziende sanno che il problema c'è, ma non tutte hanno già riconosciuto la portata di questo cambiamento. Si cerca quindi di sensibilizzarle». Anche perché, «come in tutti i processi, se si anticipa il problema lo si può affrontare in maniera efficiente ed efficace, se invece non si anticipa e si rincorre, si va incontro a diverse difficoltà». E non va dimenticato, aggiunge infine Talleri, «che la Svizzera e il Ticino non sono un'isola felice. Come tutti siamo esposti a potenziali attacchi informatici: in Ticino per esperienza diretta conosco aziende attaccate e danneggiate pesantemente da questo tipo di attacchi». Insomma, «già succede e succederà sempre di più in futuro».