I nuovi paradigmi legislativi della compliance e le difficoltà di recepimento da parte degli operatori

intervista a Corrado Giustozzi, esperto di sicurezza cibernetica presso il CERT-PA (Agenzia per l'Italia Digitale) e componente l'Advisory Group di Enisa (Agenzia dell'Unione Europea per la cybersecurity)

GDPR, Direttiva NIS, Regolamento eIDAS cambiano radicalmente il paradigma della compliance, passando dal criterio dell'adempimento a quello della responsabilizzazione degli operatori. Quali sono i presupposti del legislatore europeo per questo cambiamento epocale, soprattutto per l'Italia?

Il paradigma adottato dal Legislatore europeo per normare gli obblighi di sicurezza in determinati settori regolati, quali ad esempio i fornitori di servizi critici per la società oppure i soggetti che trattano dati personali, è effettivamente molto cambiato o per dir meglio si è assai evoluto, in questi ultimi anni.

Si è passati infatti in modo abbastanza repentino da un approccio interamente prescrittivo, basato su una logica che potremmo definire "dell'adempimento", ad un approccio finalizzato ai risultati e basato su una logica "della responsabilizzazione". Ciò significa, in termini generali, che gli operatori non devono più limitarsi a seguire passivamente le indicazioni puntuali fornite dalle Autorità di vigilanza e controllo, come avveniva in passato, ma devono divenire parte attiva nel contribuire essi stessi a definire e migliorare i propri processi dal punto di vista della compliance e del raggiungimento degli obiettivi imposti. Questo è un vero ribaltamento di prospettiva, perché il Legislatore oggi dice agli operatori "cosa devono ottenere" e non più "cosa devono fare e come", lasciando loro la libertà di decidere qual è il modo migliore per ottenere i risultati richiesti. Ciò ha comportato un certo disorientamento negli operatori, che in passato erano abituati a sentirsi dare indicazioni puntuali su come comportarsi, mentre oggi devono deciderlo da soli.

Ad esempio, in molti hanno lamentato il fatto che nelle leggi più recenti, quali il GDPR, manchino gli elenchi prescrittivi di "Misure minime" di sicurezza presenti in passato: questa tuttavia non è una dimenticanza del Legislatore ma una conseguenza diretta di questo nuovo approccio, secondo il quale è compito di ciascun operatore definire ed adottare le misure di sicurezza più idonee ed adeguate alla propria specifica situazione, derivandole da una attenta ed accurata analisi del proprio profilo di rischio.

In altre parole, il Legislatore ha finalmente riconosciuto ciò che gli esperti di sicurezza predicavano da anni: ossia che ciascun operatore è diverso dagli altri ed ha le sue proprie specificità, ed è dunque sbagliato imporre a tutti le medesime misure (minime) di sicurezza, le quali rischiano di essere insufficienti per qualcuno e sovrabbondanti per qualcun altro. L'approccio più corretto è invece quello nel quale ciascuno definisce le misure più adatte a sé, derivandole da una analisi del rischio che solo lui può fare;

prendendosi così la responsabilità dell'intero processo, dalla fase di analisi a quella di implementazione e di esercizio. Si tratta ovviamente di un approccio molto difficile da seguire, in quanto richiede una grande maturità nell'operatore, ma è l'unico a fornire risultati efficaci; oltretutto, se affrontato con serietà, non solo mette l'operatore al riparo da eventuali problemi in caso di incidente (in quanto a quel punto egli dovrà poter sostenere davanti all'Autorità di vigilanza le proprie scelte) ma, soprattutto, consente di dosare gli investimenti in sicurezza secondo criteri oggettivi, consentendo così anche di operare risparmi non indifferenti.
È importante notare infine che questo approccio è ormai adottato in tutte le recenti normative rilevanti, quali il **Regolamento (UE) 910/2014 (eIDAS)** sul mercato comune per i servizi digitali (dove riguarda i fornitori di servizi fiduciari), il **Regolamento (UE) 679/2016 (GDPR)** sulla protezione dei dati personali (dove riguarda tutti i titolari di trattamento), ed infine la **Direttiva (UE) 1148/2016 (NIS)** sull'innalzamento della sicurezza di quelle che in passato venivano chiamate "infrastrutture critiche" (dove riguarda tutti i fornitori di servizi essenziali per il funzionamento della società).

E quali sono le risposte delle funzioni interessate nel nostro Paese, dal suo punto di osservazione?
L'Italia ha prontamente messo a punto gli apparati di gestione previsti da queste normative, ad esempio costituendo le apposite Autorità nel caso della Direttiva NIS (mentre per il GDPR l'Autorità era già esistente, essendo lo stesso Garante della protezione dei dati personali), ma forse ha dato un po' per scontato che gli operatori avrebbero colto da soli la grande differenza di approccio e sarebbero stati in grado di adeguarsi prontamente ed autonomamente.
La mia sensazione è invece che gli operatori non si siano resi conto della portata del cambiamento, e delle nuove responsabilità che ora incombono su di loro, e non sappiano bene come regolarsi per rendersi conformi ai nuovi requisiti.

Quali dovrebbero essere le chiavi per divulgare in modo appropriato questo nuovo approccio e ottenere risultati positivi per la tutela delle informazioni?
Questo nuovo approccio, che rende l'analisi del rischio un elemento cruciale nella compliance di ogni operatore, non è purtroppo stato correttamente e tempestivamente divulgato e spiegato presso gli interessati. E, come al solito, sono soprattutto le imprese più piccole, quelle che non hanno una cultura specifica della sicurezza, a farne le spese, perché non sanno a chi rivolgersi per impostare un approccio corretto e finiscono magari preda di consulenti improvvisati e con pochi scrupoli.
Secondo me le associazioni di categoria dovrebbero darsi come obiettivo proprio quello di informare e formare i loro associati su questi temi, aiutandoli a crescere quel minimo necessario per dotarsi di sufficiente autoconsapevolezza e poter, magari, scegliere con cognizione di causa il miglior consulente ed il miglior percorso di adeguamento.

Quali sono le differenze più significative nelle reazioni tra le diverse generazioni?
È difficile generalizzare, tuttavia la mia impressione è che le imprese più giovani e innovative, le start-up, siano sempre più allergiche ai temi della compliance, della sicurezza e della privacy, che sono visti come inutili ed ingombranti retaggi di un passato analogico reso obsoleto dalle tecnologie digitali. In realtà è tutto l'opposto: usando male le straordinarie funzionalità messe a disposizione dalla Rete e dalla capillare diffusione delle tecnologie personali si possono recare enormi danni a terzi, siano essi i propri clienti o altri componenti della società civile (altre aziende, cittadini, eccetera). Per questo è tanto più importante che i concetti di "security by design", di analisi del rischio e di analisi di impatto, entrino a pieno diritto nel ciclo di sviluppo di tutti i prodotti e servizi, soprattutto quelli interamente digitali e network-centrici.