

L'impatto dell'accountability/4

I MEZZI A DISPOSIZIONE

Audit. Finora non è stata riconosciuta alcuna realtà

Da accreditare gli enti di certificazione

Saverio Cavalcanti
Ludovica Mosci

■ I codici di condotta di cui al nuovo regolamento privacy non sono un'assoluta novità normativa, essendo già previsti dalla direttiva 95/46/Ce e richiamati dal Codice privacy. Tali codici, promossi dalle associazioni di categoria e approvati dall'autorità di controllo, dettano le linee guida rispetto al corretto e trasparente trattamento dei dati in determinati settori, in funzione della loro specificità.

CODICI DI CONDOTTA

In Italia sono già stati adottati codici di condotta (la cui validità ed efficacia post-entrata in vigore del regolamento dovrà essere confermata), in-

di autoregolamentazione sono utili anche per ripondere a problematiche di settore

responsabilità in capo a titolari o responsabili, lasciando impregiudicati i poteri delle autorità di controllo, ma possono essere tenute in debito conto nel decidere l'ammontare di eventuali sanzioni. Lo stesso vale per l'adesione ai codici di condotta.

Certificazioni, marchi e sigilli non possono tuttavia ancora essere adottati, poiché devono provenire esclusivamente da enti certificatori approvati dal governo (dall'organismo di accreditamento Accredia) o dal Garante: questi ultimi, con una nota del 18 luglio, hanno chiarito che al momento nessun ente è stato certificato allo scopo, ma che sono in corso lavori, di concerto con le autorità Ue «per poter garantire l'avvio delle attività di accreditamento e certifica-

teralia, in ambito giornalistico, investigativo o per i trattamenti a fini statistici e scientifici.

È possibile adottare codici di condotta comunitari: di recente è stato, ad esempio, sottoposto all'esame del gruppo di lavoro Articolo 29, un codice di condotta per gli sviluppatori di app in ambito sanitario. Con il regolamento, inoltre, anche le società extra Ue a cui non si applica il regolamento potranno aderire a tali codici. Si tratta, quindi, di strumenti molto utili per fare fronte alle peculiarità di determinati settori e all'evoluzione della tecnologia.

CERTIFICAZIONI, MARCHI E SIGILLI

Assoluta novità sono invece certificazioni, marchi e sigilli, che consen-

tono alle società di dimostrare la conformità al regolamento, in linea con il principio di responsabilizzazione. Le società possono infatti sottoporsi volontariamente ad un iter di esami e controlli (audit) da parte di enti certificatori, che culminano nell'apposizione di un certificato del tipo Gdpr privacy certified, valido per un massimo di tre anni.

Le certificazioni non eliminano le

zione, nel rispetto delle scadenze previste dal regolamento».

Non resta, dunque, che attendere fiduciosi; in ogni caso, nel frattempo, come anche precisato dal Garante, nulla impedisce alle società di sottoporsi ad audit privacy e meccanismi di certificazione per dimostrare, anche in linea con le *best practice* di mercato, il rispetto della normativa.

Si pensi, ad esempio, agli standard internazionali Iso/Iec 27001 in materia di sicurezza dei sistemi informatici, nonché gli Iso/Iec 29100:2011, che si riferiscono in particolare alle operazioni effettuate con strumenti tecnologici che richiedono particolari controlli sulla privacy.

© RIPRODUZIONE RISERVATA

LE SCELTE

I codici

