PRIVACY, CAMBIANO LE NORME
COSÌ DEVE ADEGUARSI CHI FA RICERCHE DI MERCATO

Il Regolamento europeo in materia di protezione dei dati personali, in vigore dal 24 maggio 2016 e operativo dal prossimo maggio 2018, incide profondamente anche sulle attività di indagine statistica

Rosapia Farese
Ceo Medi-Pragma

Lucio Corsaro
General manager Medi-Pragma

È ufficialmente in vigore il nuovo Regolamento europeo 679/2016 in materia di protezione dei dati personali. Il testo – pubblicato sulla Gazzetta Ufficiale dell'Unione europea il 4 maggio 2016 – diventerà definitivamente applicabile in via diretta in tutti i Paesi Ue a partire dal 25 maggio 2018, quando dovrà essere garantito il perfetto allineamento fra la normativa nazionale in materia di protezione dati e le disposizioni del regolamento.
Il regolamento è parte del cosiddetto pacchetto protezione dati, l'insieme normativo che definisce un nuovo quadro comune in materia di tutela dei dati personali per tutti gli Stati membri dell'Ue e comprende anche la direttiva in materia di trattamento dati personali nei settori di prevenzione, contrasto e repressione dei crimini. La direttiva, pubblicata in Gazzetta insieme al regolamento e vigente dal 5 maggio 2016, dovrà essere recepita dagli Stati membri entro due anni.
Sul sito del Garante per la protezione dei dati personali è disponibile una pagina informativa (http://www.garanteprivacy.it/pacchettoprotezionedati) che ha illustrato finora l'iter normativo del Pacchetto e che sarà progressivamente arricchita con aggiornamenti e materiali informativi e di approfondimento.
Rispetto all'attuale Codice privacy dlgs 196/2003 è mantenuto sia l'istituto del "Titolare del trattamento" (data controller) che il "Responsabile del trattamento" (data processor), mentre è abolito l'incaricato del trattamento.
Il nuovo regolamento introdurrà una legislazione in materia di protezione dati uniforme e valida in tutta Europa, affrontando temi innovativi – come il diritto all'oblio e alla portabilità dei dati – e stabilendo anche criteri che da una parte responsabilizzano maggiormente imprese ed enti rispetto alla protezione dei dati personali e, dall'altra, introducono notevoli semplificazioni e sgravi dagli adempimenti per chi rispetta le regole. Il regolamento Ue 679/2016, però, non sarà l'unica fonte legislativa per regolamentare la protezione dei dati personali, infatti le autorità dei singoli Stati membri – e quindi il Garante della privacy per l'Italia – potranno integrare i contenuti del regolamento dettagliando meglio alcuni aspetti che al momento appaiono poco chiari, introdurre linee guida generali e di settore, regolamentare aspetti particolari, etc.
A tal proposito occorre ricordare che, con l'uscita del regolamento 679 non vengono aboliti i provvedimenti del nostro Garante su videosorveglianza, amministratori di sistema, fidelity card, biometria, tracciamento flussi bancari, etc. Tali provvedimenti probabilmente saranno modificati e/o integrati dal Garante per aggiornarli ed eventualmente adeguarli alle prescrizioni del Regolamento Europeo 679.
Il Garante italiano potrà inoltre integrare il Regolamento Ue 679 per disciplinare il trattamento di dati personali effettuato per adempiere obblighi di legge italiana e in particolari ambiti, ad esempio quello dei dati sanitari, oppure per definire in modo più dettagliato gli obblighi per le Pmi (ovvero per le organizzazioni che occupano meno di 250 dipendenti, per le quali il regolamento 679 ha stabilito delle semplificazioni).

LE PRINCIPALI NOVITÀ

Ma quali sono le principali novità per le imprese nella gestione della privacy a fronte del regolamento Ue?

L'aspetto più significativo è sicuramente il cambio di approccio rispetto al Codice privacy attualmente in vigore in Italia, e in particolare all'allegato B, ovvero al disciplinare tecnico delle misure minime di sicurezza.

Il nuovo regolamento europeo sulla privacy, infatti, non definisce requisiti specificati in termini precisi, come avviene per l'attuale normativa italiana sulla privacy, ma sposta la responsabilità di definire le misure di sicurezza idonee a garantire la privacy dei dati personali trattati sul titolare o responsabile del trattamento, dopo un'attenta analisi dei rischi.

Dunque non ci sono più misure minime, ma solo misure di sicurezza adeguate, progettate dal titolare o responsabile del trattamento dopo aver effettuato l'analisi dei rischi che incombono sui dati personali che si intende trattare. In proposito va sottolineato il fatto che le misure di prevenzione devono essere poste in atto prima di iniziare il trattamento.

Poiché a livello nazionale la legislazione italiana e il Garante per la protezione dei dati personali hanno seguito il percorso europeo, a partire dalla direttiva europea 46/95, a livello di principi sulla privacy non ci sono differenze significative tra normativa italiana e regolamento europeo. Infatti, alcune regole già imposte dal Codice privacy e dalle successive disposizioni del Garante restano valide, anche se con contorni un po' meno definiti da criteri oggettivi.

In sostanza: viene regolamentato solo il trattamento di dati personali di persone fisiche (non giuridiche) per scopi diversi dall'uso personale.

Resta una distinzione tra trattamento di dati personali comuni e trattamento di dati cosiddetti sensibili, anche se la definizione del dlgs 196/2003 non viene utilizzata nel regolamento Ue 679, lasciando però la possibilità agli Stati membri di stabilire una disciplina particolare in merito.

Restano gli obblighi di informare l'interessato sull'uso che verrà fatto dei suoi dati personali e quelli di ottenere il consenso per i trattamenti non necessari o per i trattamenti di particolari tipi di dati. Ad esempio quelli idonei a rivelare lo stato di salute delle persone, le origini razziali, le idee religiose, etc.

CHE COSA CAMBIA IN CONCRETO

Tra gli elementi che cambiano vi sono sicuramente:

- La denominazione e i ruoli degli attori: il titolare del trattamento rimane tale, il responsabile del trattamento è ora responsabile in solido con il titolare per i danni derivanti da un trattamento non corretto, l'incaricato rimane il soggetto che fisicamente tratta i dati, ma tale ruolo non è delegabile, se non attraverso uno specifico accordo contrattuale. Il responsabile può individuare un proprio rappresentante.
- I dati personali trattati devono essere protetti con misure organizzative e tecniche adeguate a garantirne la riservatezza e l'integrità.
- I diritti dell'interessato sono più ampi e maggiormente tutelati.
- Il responsabile del trattamento deve mettere in atto misure tecniche ed organizzative tali da consentirgli di dimostrare che tratta i dati personali in conformità al regolamento.

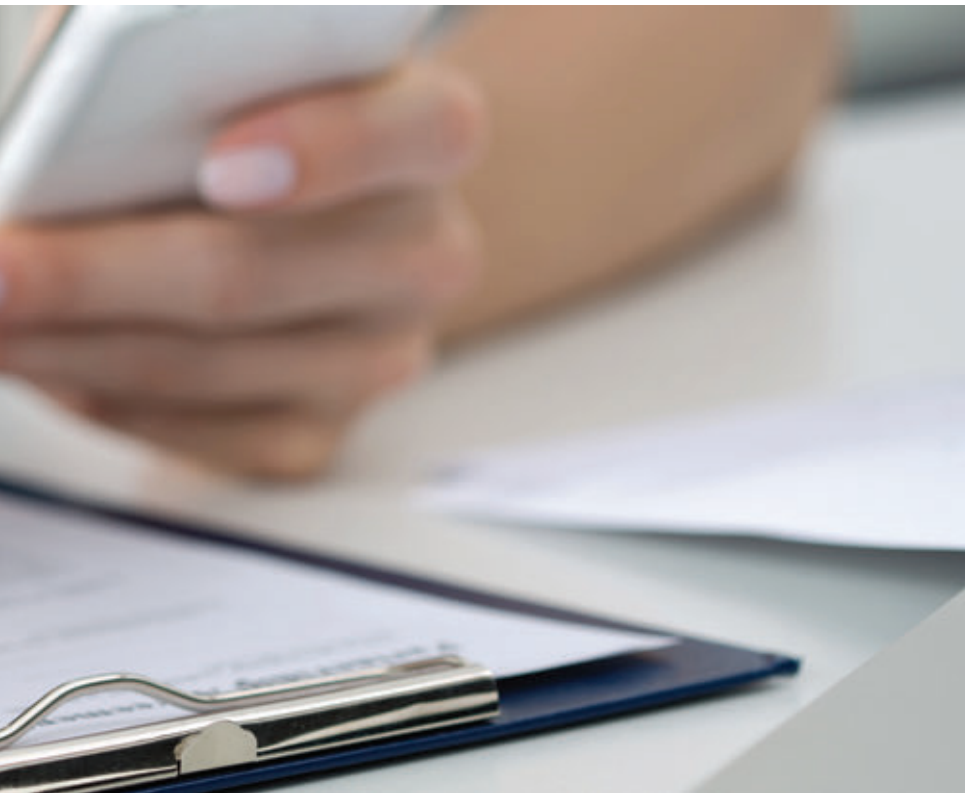
Tali misure devono seguire lo stato dell'arte e devono derivare dall'analisi dei rischi che incombono sui dati, secondo relativa gravità e probabilità.

Altre novità riguardano la cosiddetta privacy by default e la privacy by design. Nel primo caso devono essere trattati "per default" solo i dati necessari a perseguire le finalità del trattamento posto in essere dal responsabile dello stesso, ovvero non devono essere trattati dati in eccesso senza che una persona fisica autorizzata lo consenta.
Nel secondo, ogni nuovo trattamento di dati personali dovrà essere progettato in modo da garantire la sicurezza richiesta in base ai rischi cui è sottoposto prima di essere implementato. Anche i sistemi informatici dovranno essere progettati secondo tale principio.
Possono esserci più responsabili per un medesimo trattamento che risulteranno, pertanto, corresponsabili di eventuali trattamenti non conformi, ma dovranno stabilire congiuntamente le rispettive responsabilità.
Le imprese con sede al di fuori dell'Unione europea, che trattano dati personali di interessati residenti nella Ue dovranno eleggere una propria organizzazione o entità all'interno della Ue che sarà responsabile di tali trattamenti.
Devono essere mantenuti registri dei trattamenti di dati effettuati con le informazioni pertinenti e le relative responsabilità. Tali registri non sono obbligatori per organizzazioni con meno di 250 dipendenti salvo che non trattino dati sensibili (secondo la definizione del Codice della privacy attualmente in vigore) o giudiziari. Tale discriminante potrà essere meglio specificata da appositi provvedimenti del nostro Garante.
Il responsabile del trattamento deve notificare all'autorità competente e, in casi gravi, anche all'interessato – ogni violazione dei dati (data breach) trattati entro 72 ore dall'evento.
Quando un trattamento presenta dei rischi elevati per i dati personali degli interessati (i casi specifici dovranno essere esplicitati dall'Autorità Garante), il responsabile del trattamento deve effettuare una valutazione di impatto preventiva, prima di iniziare il trattamento.
Viene introdotta la certificazione del sistema di gestione della privacy (le cui modalità dovranno essere meglio definite tramite gli organismi di accreditamento europei, Accredia per l'Italia).

È richiesta la designazione di un responsabile della protezione dei dati (data protection officer) nelle aziende pubbliche e nelle organizzazioni che trattano dati sensibili o giudiziari su larga scala oppure che la tipologia di dati trattati e la loro finalità richieda il controllo degli incaricati al trattamento su larga scala.
Proprio quest'ultimo punto, variato rispetto alle precedenti versioni del Regolamento, farà molto discutere, poiché non stabilisce criteri precisi e oggettivi (cosa significa "su larga scala"?) per l'adozione di tale figura professionale, di competenze adeguate a garantire una corretta applicazione della normativa sulla privacy. Il responsabile per la protezione dei dati dovrà essere correttamente informato dal responsabile del trattamento su tutte le attività che riguardano la privacy e dovrà disporre di risorse adeguate per svolgere il proprio compito e mantenere le sue competenze adeguate al ruolo che ricopre. Egli dovrà inoltre essere indipendente dalle altre funzioni dell'organizzazione e riferire solamente all'alta direzione.
La sicurezza dei dati – in termini di riservatezza, integrità e disponibilità – deve essere garantita in funzione del rischio che corrono i dati stessi, dei costi delle misure di sicurezza e dello stato dell'arte della tecnologia. Pertanto le password di almeno otto caratteri variate almeno trimestralmente, l'antivirus aggiornato, il firewall e l'aggiornamento del sistema operativo potrebbero essere misure adeguate per determinati trattamenti, ma non per altri, oppure in determinate organizzazioni, ma non in altre. In ogni caso lo potrebbero essere oggi, ma non domani quando il progresso tecnologico (anche degli hacker e di coloro che minacciano i nostri dati) potrebbe renderle insufficienti.

SERVE UN CAMBIO DI MENTALITÀ

Lasciando per il momento stare gli impatti che il nuovo regolamento Ue potrà avere sulla privacy per i colossi del web, quali Facebook, Google, etc., è opportuno osservare che nelle piccole e medie imprese italiane dovrà cambiare l'approccio alla privacy, soprattutto per quelle organizzazioni che trattano dati



sensibili o giudiziari. Occorrerà un cambio di mentalità: non bastano più un po' di carte (informative, consensi, lettere di incarico, ...) e alcune misure minime di sicurezza specifiche (password, antivirus,...) per garantire il rispetto della legge. Poiché molti imprenditori vedono la privacy solo come un disturbo da gestire soltanto per non incorrere in sanzioni e, quindi, come una pratica da sbrigare nel modo più indolore possibile, ecco che il passaggio al nuovo regolamento – che dovrà avvenire nel prossimo anno – non sarà proprio una passeggiata.

Le responsabilità in capo al responsabile del trattamento (ex titolare del trattamento) sono maggiori e comunque più impegnative da gestire, soprattutto laddove il trattamento di dati venga delegato a fornitori (es. consulenti del lavoro, consulenti fiscali e legali, strutture esterne, etc.) che dovranno inevitabilmente essere tenuti sotto controllo.

Non è che taluni principi fossero assenti dalla normativa italiana del 2003, ma – complice la crisi e le semplificazioni adottate da precedenti governi, soprattutto l'abolizione del Dps – hanno un po' sminuito l'importanza della privacy in azienda, anche perché – probabilmente – sono state molto rare le sanzioni comminate alle aziende, e i controlli poco frequenti. Paradossalmente ha spaventato di più la disposizione sui cookie perché la sua mancata applicazione è di fatto pubblica, mentre altre regole di fatto trascurate rimangono tra le mura delle organizzazioni di ogni dimensione.

PROSPETTIVE FUTURE

L'indeterminatezza di alcune regole potrà essere colmata da disposizioni specifiche dei singoli Stati membri e/o da linee guida di settori specifici che potranno agevolare l'interpretazione della legge.

Per certi versi la privacy sarà meno materia per avvocati – se non per la stesura di contratti che regolamentano i rapporti fra clienti e fornitori anche in materia di trattamento dati personali – e più materia per esperti della sicurezza delle informazioni. Infatti l'approccio del nuovo regolamento europeo sulla privacy si avvicina, mutatis mutandis, a quello della norma Uni En Iso/Iec Iso 27001 e della linea guida Uni En Iso/Iec Iso 27002.

L'adozione del nuovo regolamento Ue sarà, pertanto, più impegnativa per piccole organizzazioni che trattano molti dati sensibili o giudiziari, quali organizzazioni private nel campo della sanità (cliniche ed ambulatori privati, farmacie, ...), studi di consulenza del lavoro, infortunistiche, studi legali, studi di consulenza fiscale, etc., piuttosto che per aziende che trattano come unici dati sensibili i dati relativi ai propri dipendenti. Anzi saranno proprio queste ultime che dovranno pretendere da società e studi di consulenza esterna adeguate garanzie per il trattamento dei dati di cui sono responsabili.

TRA VERA RICERCA E MARKETING DIRETTO

Va posta attenzione sulle ricerche di mercato e sulla confusione che spesso le accomuna sotto il tetto di marketing diretto. Ovvero distinguendo tra studi realizzati secondo i principi della statistica e della ricerca scientifica, applicata con esclusiva finalità di studio e conoscenza dei fenomeni sociali, senza riferimento a dati o comportamenti individuali, e quelle attività che, anche ove si avvalgano di tecniche di ricerca, sono finalizzate ad azioni di marketing diretto su persone identificate nominativamente. La caratteristica che distingue le ricerche di mercato dal marketing diretto, è quella di essersi data da tempo un codice di autodisciplina che vieta l'attività di direct marketing e di non ritenere essenziale l'identificazione del soggetto intervistato.

Nelle indagini socio-demografiche, infatti, i dati identificativi vengono raccolti solo per poter effettuare i controlli di qualità sulla rilevazione, al termine dei quali vengono distrutti, e i risultati statistici sono prodotti su dati rigorosamente anonimi.

A queste indagini conoscitive viene riconosciuta un'utilità sociale e pertanto si applica il Codice per la statistica e la ricerca scientifica siglato dal Garante, dall'associazione di settore (Assirm) e da altri enti rappresentativi della comunità scientifica.

Parzialmente più complessa, ma comunque prevista dal predetto codice, è la situazione relativa alle ricerche continua-

tive o su panel per le quali è necessario conservare i dati personali al fine di poter reintervistare gli stessi soggetti.
In questo caso, infatti, è necessario il consenso informato degli interessati a tal fine ci sono tre momenti che caratterizzano l'attività di questo settore.
La parte iniziale del processo di ricerca, nella quale si può operare liberamente, che consiste nell'acquisizione di liste di cittadini o imprese da intervistare su cui effettuare la ricerca. Poi c'è la fase di contatto diretto con l'interlocutore, ed è questa la fase su cui maggiormente impatta la legge sulla privacy perché si raccolgono informazioni che sono temporaneamente abbinate ai dati identificativi degli interessati. In questa fase bisogna attenersi alle norme previste dalla legge e dal codice. Infine c'è la fase di elaborazione statistica dei dati e della sintesi dei risultati che, essendo effettuata su dati resi anonimi, non pone particolari problemi.

UNA DIFFERENZIAZIONE NECESSARIA

Diverse sono le procedure e le norme che si applicano al direct marketing e per questo gli esperti concordano nel ritenere che la confusione tra le due attività sia penalizzante per il mondo delle ricerche di mercato. Il primo obiettivo per il settore di ricerca di mercato deve essere quello di sganciarsi dall'involontaria coabitazione con il direct marketing. Bisognerà fare cultura in questo senso e creare delle distinzioni. È anche errato muoversi in modo monolitico perché esistono statistiche e sondaggi che vanno disciplinati in maniera diversa dagli altri. In questo senso ci sono altre possibilità, proposte da Asseprim, federazione nazionale che rappresenta le aziende di servizi professionali per le imprese in seno a Confcommercio, per sostenere nelle sedi opportune le richieste di modifica della norma avanzate dalle società di ricerca.
Assirm, che raggruppa i maggiori istituti italiani di ricerche di mercato, sondaggi di opinione e ricerca sociale, sottolinea come l'aver sottoscritto con il Garante il codice della ricerca scientifica e della statistica, costituisca un primo riconoscimento ufficiale del reale status della ricerca di mercato e sociale e della sua utilità per lo sviluppo e la crescita di una società democratica. L'associazione ribadisce l'importanza di attenersi rigorosamente alle norme del codice per rafforzare il riconoscimento già acquisito ed evitare che la ricerca venga impropriamente associata ad altre indagini. Per far ciò occorre differenziarla nettamente dalle attività di marketing e comunicazione diretta e diffonderne internazionalmente la giusta immagine.
Le norme di autodisciplina possono svolgere un ruolo importante in questo ambito e Assirm con le equivalenti associazioni europee si sta adoperando in tal senso, sviluppando e implementando regole rivolte a disciplinare la possibile intrusività della tecnologia, ad esempio in relazione all'uso dei sistemi di chiamata automatica o alla condivisione di liste dei cittadini che richiedono di non essere contattati (opt-out lists).

IL VALORE DELLA RICERCA:

Il rispetto delle norme e dei codici, legali e deontologici, non sono limiti che opprimono i ricercatori e/o gli istituti di ricerca. Piuttosto rappresentano confini che, se si rispettano, garantiscono il valore della ricerca per chi la compra, salvaguardando le persone che sono "oggetto" della ricerca stessa. Un valore che crea reale sostenibilità nel tempo per l'intero ecosistema di stakeholder della ricerca. Il codice è stato costituito soprattutto nel interesse degli istituti e dei suoi clienti.
Il mercato e il marketing a livello globale sono sempre più complessi e sempre più il customer è al centro delle strategie aziendali. Oggi il mantra nelle direzioni aziendali è "value-based marketing" un approccio al mercato che richiede di fornire valore al cliente, creare e gestire relazioni in modo che i benefici siano godibili da tutta la filiera.
Il supporto alla creazione e alla gestione di tale value chain richiede il supporto continuo ed accurato di informazioni e l'applicazione di differenti metodologie di indagini e interpretazioni. Le aziende devono monitorare, alcune in continuo, e adeguare velocemente la propria value-proposition e farlo mettendosi nei panni dei loro clienti. Per fare ciò esistono le opportune tecniche, non sempre già disponibli all'interno delle strutture aziendali.

Parole chiave
Sicurezza dati, privacy, ricerche di mercato, Regolamento europeo 679/2016
Aziende/Istituzioni
Unione europea, Garante privacy, Medi-Pragma, Assirm, Asseprim, Confcommercio

