

Privacy e azienda: la chimera della non applicabilità.

Nonostante l'opinione comune che vuole che le aziende ricadano fuori dall'ambito di applicazione del Regolamento Europeo, salvo il caso in cui il nome della società identifichi una persona fisica o se il "dato di contatto" della persona giuridica rappresenti un nome e un cognome di una persona fisica ed allora le informazioni inerenti persone giuridiche possono considerarsi "concernenti" persone fisiche e in tal caso possono ricadere comunque nell'ambito di applicazione, occorre fermarsi a considerare che la raccolta di dati societari in cui sono presenti dati di persone fisiche (soci consiglieri, etc.) fa invece rientrare completamente l'azienda nell'ambito della gestione completa del GDPR.

L'exkursus che porta a queste considerazioni è presto illustrato:

l'ambito di applicazione del Regolamento europeo è chiaramente espresso:

all'articolo 1 che "stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali..... protegge i diritti e le libertà fondamentali delle persone fisiche in particolare il diritto alla protezione dei dati personali";

all'art. 4 definisce dato personale come "qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato). Si considera identificabile la persona fisica...";

al considerando 14, ove si afferma "È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali.

Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto”.

Le prime indicazioni ci vengono già dal Working Party art.29, parere 4/2007 dove nel definire il concetto e la portata di dato personale, si fanno alcune ipotesi e si giunge a considerazioni molto più cautelative nei confronti della tutela dei dati personali riferibili a persone giuridiche. Testualmente “... le informazioni sulle persone giuridiche non sono in linea di principio disciplinate dalla direttiva, e quindi non godono della protezione da questa disposta. Ciò nondimeno, alcune norme di protezione dei dati possono, in certe circostanze, applicarsi indirettamente alle informazioni concernenti imprese o persone giuridiche”.

E, più in particolare, il medesimo Working Party, nel suddetto parere aveva esplicitamente affermato che le informazioni sulle persone giuridiche possono considerarsi “concernenti” persone fisiche in virtù della loro situazione specifica “È quel che accade quando il nome di una persona giuridica deriva dal nome di una persona fisica, oppure nel caso dell’indirizzo e-mail di un’impresa di norma usato da un dato dipendente, o delle informazioni su una piccola impresa (giuridicamente un “oggetto” piuttosto che una persona giuridica) che possono descrivere il comportamento del suo titolare. In tutti questi casi, in cui i criteri di “contenuto”, “finalità” o “risultato” fan sì che le informazioni su una persona giuridica o su un’impresa possano considerarsi come “concernenti” una persona fisica, è opportuno considerare tali informazioni come dati personali e si applicano le norme di protezione dei dati.” (WP29, dal Parere 4/2007 sul concetto di dati personali del WP29).

Sul tema il Garante era già intervenuto subito dopo l’entrata in vigore dell’art. 40, secondo comma, del decreto legge n. 201 del 6 dicembre 2011 che aveva determinato l’esclusione

del trattamento dei dati relativo alle persone giuridiche, enti ed associazioni dall'ambito di applicazione del Codice privacy.

In quel provvedimento il Garante argomentava il permanere della tutela in capo alle imprese facendo leva su concetto di "contraente" cui fa riferimento il Codice delle comunicazioni elettroniche nulla distinguendo dal fatto che siano o no essi persone fisiche o giuridiche. Pertanto, questi ultimi soggetti "continueranno a fruire della tutela prevista dal titolo X del codice della privacy per gli abbonati a servizi di comunicazione elettronica".

Dubbi eventualmente venuti meno con l'art. 1, comma 7, lett. a), n. 3 del d.lgs. 69/2012 che sostituendo il termine "interessato", con quello di "contraente o utente" ha reso applicabili quelle previsioni anche alle persone giuridiche.

Da ultimo l'intervento del decreto legge 18 aprile 2019, n. 32, convertito con modificazioni, in legge 14 giugno 2019, n. 55 che all'art.1, lettera a), che al di là di ogni ragionevole dubbio, definitivamente riformula la definizione di contraente qualificandolo come la "persona fisica o giuridica che sia parte di un contratto con il fornitore di servizi di comunicazione elettronica accessibili al pubblico, per la fornitura di tali servizi".

Detto quanto sopra che illumina su come sia labile il detto *il GDPR non coinvolge le aziende*, in ogni caso osserviamo che le aziende devono comunque rispettare alcune regole di ~~ingaggio~~ che, per brevità, si sintetizzano nei seguenti sei punti:

- Registro dei Trattamenti
- Informativa
- Lettere di Designazione
- Procedure
- Registro Data Breach

▪ DPIA Data Protection Impact Assessment

A maggior ragione l'impianto su esposto è necessario qual ora un'azienda acquisisca dati di altre aziende (bilanci, visure, conti correnti del sistema bancario, etc.) per fare analisi e clusterizzazioni.

Anche perché solitamente in queste acquisizioni troviamo anche i dati dei soci, del management, delle persone affini, identificando in questo caso la necessità di rispettare completamente il codice.

Ma il problema è poi anche la conservazione ed archiviazione di quei dati che richiede importanti misure tecnologiche e di impianto.

Oggi il problema è che nella convinzione che il GDPR non si applica alle aziende le stesse stiano prendendo delle gran cantonate trascurando invece l'applicazione corretta del GDPR ai loro processi.

Facciamo un esempio:

l'azienda A prende i dati camerali dell'azienda B e li utilizza per fare dei sistemi di analisi incrociata di mercato per poter personalizzare il prodotto che A offre a B.

Per far ciò A usa un outsourcer esterno C a cui passa i dati di B.

Ovviamente per personalizzare al meglio i prodotti A chiede anche i dati dei dipendenti e dei soci di B.

L'azienda A è tranquilla perché ritiene di non essere nel GDPR lavorando con l'azienda B (quindi azienda su azienda) e che i dati camerali essendo pubblici non rientrano nel GDPR.

Questo è un tipico errore di valutazione in quanto si incorre nelle seguenti problematiche:

mancata compilazione del registro dei trattamenti da parte di A.

I dati aziendali di B devono poi essere conservati e tale conservazione ricade su A con tutti i requisiti di sicurezza del caso, inoltre essendo passati a C occorre comunque garantire che i dati siano utilizzati per la finalità per cui vengono acquisiti e conservati a norma (dpia?).

Ed ancora è necessario chiarire bene tutti i flussi organizzativi ai fini della corretta informativa e probabilmente, nel caso citato, è anche necessario svolgere una dpia da parte del titolare del trattamento.

Ma ancora peggio sono poi i dati dei soci e dei dipendenti che vengono acquisiti al fine della personalizzazione del prodotto di A per B, questi dati non rientrano nel considerando 14 succitato perché la persona fisica che rientra nei dati di contatto non può comunque essere utilizzata per altre finalità se non quelle di contatto e comunque le stesse possono essere al limite due o tre ma non certo tutti i soci, che peraltro spesso non hanno nemmeno la rappresentanza legale della società e quindi non possono essere considerate persone di contatto.

Occorre considerare che anche i dati dell'azienda, soprattutto se riferiscono ai soggetti fisici dell'azienda, quali ad esempio i debiti verso soci o lo scoring creditizio legato ai soggetti societari, identificando un comportamento, anche se solo finanziario, rientrano nei dati da tutelare.

In questo banale esempio l'azienda A si troverebbe ad essere in palese violazione di tutto l'impianto del GDPR.

E' bene infatti cristallizzare che i dati identificativi della persona giuridica ex se, sono distinti dai dati identificativi delle persone fisiche in ogni modo afferenti la persona giuridica (soci, addetti, *et similia*).

Se, pertanto, alcun limite - se non quello, comunque, afferenti il più generale diritto alla personalità ed all'identità, riconosciuto anche in favore degli Enti - incontrerà il trattamento dei dati propri delle persone giuridiche (es. denominazione, sede, dati fiscali) dovranno invece osservarsi le disposizioni del regolamento UE con riferimento ai dati delle persone fisiche collegate all'Ente.

In ultimo l'errore finale quasi decisivo è la nomina di un DPO interno da parte dell'azienda.

La figura del D.P.O. introdotta dal GDPR 679/2016 ha una funzione complessa a metà tra il consulente ed il controllore.

Il DPO svolge principalmente un ruolo di informazione e sorveglianza che è sostanzialmente affine alle attività tipiche della consulenza specialistica.

Nel mondo delle aziende questo tipo di figura è abbastanza poco conosciuta, forse solo l'R.SP.P. ha una qualche similitudine per chi opera, ma a differenza di quest'ultimo il DPO ha anche un ruolo di garanzia nei confronti dell'organismo di controllo nazionale, ovvero il garante della Privacy.

La scelta del DPO da parte delle aziende diviene quindi un elemento di particolare complessità perché non è meramente legato al "prezzo", ma bensì ad una serie di considerazioni che lo rendono particolarmente difficile da identificare in modo semplice.

Il GDPR vuole il DPO indipendente dall'organizzazione che deve vigilare, competente sulla materia normativa, esperto dell'azienda che deve servire.

La scelta di un DPO interno già non può garantire il primo punto ovvero quello dell'indipendenza, ma nemmeno molto il secondo, pertanto risponderebbe solo al terzo punto.

Questo brevissimo punto di osservazione dovrebbe consigliare a tutte le aziende una scelta esterna, che in realtà non viene fatta per una motivazione meramente economica.

Anche questa ultima valutazione è comunque facilmente smontabile solo con il considerare il costo di un eventuale errore in tema di protezione di dati personali.

Non importa quanto sia strutturata un'azienda: il Regolamento Europeo coinvolge tutti, senza distinzione.

La media delle sanzioni erogate a livello europeo si attesta sulle 30.000 euro, in alcuni casi arrivando a importi singoli di oltre 500.000 euro.

Facciamo alcuni esempi:

Il Garante austriaco ha condannato un imprenditore al pagamento di un'ammenda pari a €4.800 per aver installato le telecamere di videosorveglianza fuori dal suo esercizio commerciale, riprendendo parte del marciapiede. La palese violazione del principio di liceità, correttezza e trasparenza giustifica l'intervento del Garante. I casi riportati confermano il valore prescrittivo della normativa e la doverosa compliance al contenuto.

Il Garante privacy italiano invece è stato chiamato in causa per multare un medico, a causa di un trattamento illecito di dati personali. Sono stati utilizzati gli indirizzi di 3.500 pazienti per inviare lettere a sostegno di un candidato alle elezioni del 4 marzo del 2018, senza che gli interessati avessero espresso il consenso. 16.000€

Il Garante privacy danese ha sanzionato la società produttrice di mobili IDdesign per €200.850, corrispondenti a 1,5 milioni di corone danesi, per aver conservato i dati di un elevato numero di clienti per un periodo superiore al necessario

Il Garante privacy rumeno ha multato Unicredit Bank S.A, con un'ammenda di €130.000, per non aver adottato le giuste misure tecniche e di sicurezza in seguito all'entrata in vigore del GDPR.

L'Autorità italiana ha segnalato l'iscrizione a ruolo di 779 contravventori che porterà ad una riscossione complessiva di circa 11 milioni di euro.

Ma il Garante si mantiene attivo: a breve si concluderà l'iter per l'iscrizione di altri 500 trasgressori.

Un DPO esterno oggi costa da 10.000 euro a 80.000 euro in base alla complessità dell'azienda.

Senza contare che affidare all'esterno il ruolo di DPO è anche segno di trasparenza e qualità, mentre ricevere una multa da Garante potrebbe distruggere l'intera credibilità dell'azienda sul mercato.

Il Team Privacy

controllerprivacy.it

Corrado Faletti, Roberto De Duro, Andrea Caristi