Quando la privacy è un rompicapo

scritto da goal | 7 Agosto 2018

di Paolo Soro*

La recente entrata in vigore del nuovo regolamento sulla tutela dei dati personali (privacy), impone alcune riflessioni sulle inevitabili e – per certo verso – imponderabili ripercussioni che si stanno generando in tutti i settori. Dal 25 maggio 2018, vige il nuovo Regolamento UE 679/2016 sulla privacy (GDPR – General Data Protection Regulation), pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016. Per l'esattezza, si tratta del Regolamento del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la Direttiva 95/46/ CE (Regolamento Generale sulla protezione dei dati). Nonostante il periodo di due anni concesso per provvedere all'adeguamento da parte di ogni Paese membro, a tutt'oggi, in Italia, non è stato ancora varato il quadro normativo di riferimento nazionale. La data entro cui sarebbe scaduta la delega affidata al Governo per armonizzare le disposizioni nazionali sulla privacy, inizialmente prevista per il 21 maggio, è stata prorogata al 21 agosto 2018, ma non può escludersi che anche questa seconda scadenza verrà disattesa. Di conseguenza, per ora, si deve fare riferimento alle norme di cui al suddetto Regolamento UE, posto che lo stesso ha immediata applicazione in tutti gli Stati membri, senza necessità di alcuna espressa ulteriore norma di ratifica interna. Norma che, viceversa, sembrerebbe particolarmente importante, onde fornire perlomeno dei chiarimenti operativi in merito a determinate previsioni per nulla intellegibili: prima fra tutte, quella concernente l'eventuale obbligo di nomina dell'RPD – Responsabile della Protezione dei Dati,

anche denominato DPO – Data Protection Officier.

Occorre innanzitutto evidenziare che data l'enorme importanza che riveste al giorno d'oggi la tutela della riservatezza dellepersone, specificatamente con riguardo al trattamento e alla circolazione dei loro "dati sensibili", vi è l'assoluta necessità di una normativa in grado di garantire detta privacy. Orbene, se è pur vero che tutto è perfettibile, il Regolamento in questione appare oggettivamente ben lungi dall'essere meramente perfettibile, anche in considerazione del fatto che il Legislatore ha agito sulla falsa riga di analoghe leggi previgenti che fungevano da traccia. E' quindi ragionevole supporre che sulla materia questi debba nuovamente intervenire, appena l'attuazione pratica dello stesso Regolamento consentirà di definire l'area dell'intervento di miglioramento, con la fattiva collaborazione di tutti i soggetti competenti.

A mero titolo di esempio, elenchiamo di seguito alcuni fatti meritevoli di approfondimento per il suddetto intervento di miglioramento.

Fatto n. 1: <u>Efficacia del Regolamento</u>

È indubbio che la bontà di una legge sia direttamente proporzionale al livello di efficacia che la stessa dimostra di avere nella pratica. Il Regolamento serve a proteggere la privacy delle persone; dunque, il primo indizio determinante per esprimere un giudizio positivo circa l'utilità delle nuove regole introdotte, è verificare se, a seguito dell'entrata in vigore, si incomincino già a notare dei cambiamenti – superfluo precisarlo – in meglio, rispetto al periodo pregresso. Invero, di cambiamenti ve ne sono non pochi. In quanto "fornitori", tutti abbiamo dovuto perlomeno mettere mani alle varie informative, rivederle e ritrasmetterle ai clienti; i più attenti hanno modificato il loro sistema di archiviazione e gestione dati; per non parlare di chi (oramai, la stragrande maggioranza di noi) ha un sito Internet. In

quanto “clienti”, abbiamo dovuto modificare il nostro “consenso informato” (spesso, ristampando il nuovo documento, firmandolo una seconda volta e ritrasmettendolo a chi di dovere); abbiamo, poi, cambiato le varie credenziali/password di accesso ai tanti siti in cui siamo soliti “navigare” (anche quelli relativi a mailing list concernenti esclusivi approfondimenti professionali, per il solo fatto che vi sono inseriti i nostri recapiti personali). Acosa sono serviti questi cambiamenti? Alzi la mano chi ha – per esempio – visto diminuite le mail- spam, o le telefonate da parte delle società che propongono nuovi contratti commerciali per le utenze domestiche o business, le attività di trading online etc. I comportamenti maggiormente bislacchi restano, peraltro, quelli delle compagnie telefoniche: prima mandano una comunicazione in perfetta osservanza del Regolamento, dal seguente tenore: *“La nostra società affronta con molta serietà il problema privacy…”*, dopo, chiamano a un cellulare (il cui numero non dovrebbe essere noto ad alcuno) per proporre passaggi da un gestore all’altro, mantenendo l’attuale numero. Cosa che, a pensarci bene, ufficialmente, dovrebbe essere impossibile, posto che tutti gli interessati si erano a suo tempo assicurati di barrare la specifica casellina *“nego il consento a fornire il mio numero per attività di marketing et similia”*. Ergo, o tali compagnie telefoniche hanno una specie di gentlemen’s agreement in forza del quale si scambiano liberamente fra di loro le utenze dei propri clienti, oppure esiste una sorta di banca dati nazionale dei numeri telefonici e degli indirizzi email, a cui tali compagnie hanno accesso. Eppure, tali banche dati, dovrebbero essere sottoposte a stretta vigilanza da parte delle Autorità pubbliche. Evidentemente, questi organismi statali non devono ancora essersi adeguati alle previsioni del Regolamento UE (così come, d’altronde, non si erano mai adeguati neppure alle precedenti normative in vigore). La domanda sorge spontanea: ma il Garante della Privacy cosa fa?

In conclusione del “Fatto n. 1”, possiamo affermare che il

Regolamento ha causato molti cambiamenti; nessuno dei quali in meglio. Dunque, quanto a efficacia, il Regolamento meriterebbe una "revisione".

Fatto n. 2: <u>Facilità e costi di attuazione</u>

Un secondo pregio che ogni legge dovrebbe possedere è, poi, quello relativo alla circostanza che risulti semplice adempiere alle sue previsioni, e che le stesse non comportino dei costi sproporzionati. Ebbene, quanto ai costi, il risicato utile di gestione che di questi tempi solo poche imprese riescono a conseguire, subirà inevitabilmente una riduzione a seguito delle prescrizioni imposte dal Regolamento UE. Intanto, sarà necessario pagare un consulente specializzato che analizzi la situazione e illustri all'imprenditore o al management aziendale tutte le misure da adottare. Oltre a ciò, parimenti indispensabile sarà acquisire dei nuovi software che siano in condizione di rispondere alle raccomandazioni imposte per il trattamento dei dati. Poi, occorrerà rivedere l'intero modus operandi aziendale, di modo da attuare le nuove prescrizioni normative. A titolo di esempio: non basta essere in grado di rispondere tempestivamente alle eventuali richieste dei vari interessati, relativamente al tipo di trattamento effettuato; ma occorre poter pure dimostrare che esistono in azienda delle procedure standard già predisposte in modo tale da attivarsi immediatamente e autonomamente all'occorrenza, senza necessità che vi sia l'intervento umano. Il tutto deve inoltre essere dettagliatamente riportato nella check-list di auto-valutazione e altresì periodicamente indicato nel Registro delle attività del trattamento. La mera presenza di tutta la documentazione regolarmente annotata, fine a sé stessa non è sufficiente, ma occorre anche dimostrare che l'impresa assume nella pratica concreti comportamenti proattivi al fine di tutelare i dati degli interessati (siano essi clienti, fornitori, collaboratori o dipendenti). In realtà gli adempimenti comprendono anche le attività di formazione dei lavoratori subordinati con

l’obbligo di dimostrare ai soggetti ispettivi che gli stessi lavoratori abbiano effettivamente frequentato i corsi di istruzione e/o aggiornamento, conseguendo, ove previsto, i titoli di abilitazione del caso. Last but not least, l’imprenditore o il management aziendale deve fare attenzione ancheallanominadiun Responsabileesterno per il trattamento dei dati, diverso dal titolare del trattamento, oltre che dai contitolari del trattamento, opportunamente nominati mediante accordo scritto, nel caso in cui il titolare non possa essere sempre reperibile, con una *probabile* spesa accessoria.

Ad abundantiam, giova ricordare che il titolare e il responsabile del trattamento (o i loro rappresentanti), a richiesta, hanno l’obbligo di cooperare con l’Autorità di controllo nell’esecuzione dei suoi compiti, nonché l’onere di notificare immediatamente ogni possibile violazione. Tralasciamo volutamente le problematiche connesse al trasferimento dei dati degli interessati all’estero.

In base alle informazioni disponibili sembra che applicare il Regolamento non sia facile né a “buon mercato”. E ancora non abbiamo fatto alcun accenno a talune previsioni completamente inattuabili, oltre che di difficile comprensione, come la pseudonimizzazione, tecnica che consiste nel conservare i dati in una forma che impedisce l’identificazione del soggetto senza l’utilizzo di informazioni aggiuntive, ma sulla quale le informazioni disponibili sono ben poche. Inoltre appare quanto mai contraddittorio prima prescrivere l’obbligo di sostituire i nominativi dei soggetti (es. clienti) con dei numeri, in modo che non siano immediatamente identificabili, e poi precisare che in realtà tale obbligo non sussiste (sic). Facendo un esempio concreto, negli studi professionali risulterà assai arduo gestire le informazioni di un cliente se, ogni volta, sarà necessario che il titolare del trattamento ne ricerchi il nickname accedendo al Registro sul qual è indicato lo pseudonimo che è stato attribuito al cliente.

Possiamo concludere che, pure con riferimento al “Fatto n. 2”, il Regolamento appare migliorabile.

Fatto n. 3: <u>Congruità del regime sanzionatorio</u>

Un terzo indiscutibile fattore di valutazione afferente qualsivoglia nuova legge, riguarda la corretta gradualità e proporzionalità dell’apparato sanzionatorio, previsto dal Legislatore a fronte delle eventuali violazioni normative. Orbene, detto ulteriore elemento valutativo, anziché salvarlo, infligge il definitivo colpo di grazia al nuovo Regolamento UE. Fermo impregiudicato ogni eventuale diritto di ciascun interessato al risarcimento dei danni personali eventualmente subiti, per le violazioni del Regolamento – anche dovute solo a colpa

- sono imposte sanzioni amministrative pecuniarie che vanno:
- fino a 10.000.000,00 (dieci milioni) di euro, e, per le imprese, fino al 2% del fatturato mondiale totale annuo dell’esercizio precedente, se superiore;
- ovvero, a seconda del tipo di violazioni riscontrate:
- fino a 20.000.000,00 (venti milioni) di euro e, per le imprese, fino al 4% del fatturato mondiale totale annuo dell’esercizio precedente, se superiore.

Da questa prima analisi si può legittimamente affermare che il nuovo Regolamento UE in materia di privacy è una legge di difficile applicazione; si dovrà anche vedere se e in che misura le sanzioni previste saranno applicate, ci auguriamo in modo più efficace di quanto accaduto recentemente al capo di Facebook (Mark Zuckerberg), il quale, in audizione dinnanzi al Parlamento europeo sulla prima clamorosa fuga di notizie e uso illegittimo dei dati personali da parte del gestore di una delle applicazioni social più diffusa al mondo, se l’è di fatto cavata solo con delle scuse. Quindi, la linea di difesa che, a questo punto, potranno seguire i titolari e/o i responsabili del trattamento di dati sensibili, in caso di

fuga di notizie o uso improprio dei dati gestiti, potrebbe essere: *Privacy? I am sorry!*

* ***Odcec Roma***