Dati personali: il Gdpr 4 anni dopo

Autore: Fabio Di Nunno

Fonte: Città Nuova

Ricorrono i 4 anni dall'applicazione del Regolamento generale sulla protezione dei dati dell'Ue: scopriamo come l'Europa aiuta a mantenere il controllo dei nostri dati personali nel mondo digitale

Il **Regolamento generale sulla protezione dei dati** (Gdpr) dell'**Unione europea** (Ue) è entrato in vigore 4 anni fa, il 25 maggio del 2018. La **Commissione europea** ha presentato una relazione sulla valutazione e la revisione del regolamento a giugno 2020 e la prossima valutazione è prevista per il 2024. Il Gdpr ha lo scopo di **proteggere le persone quando i loro dati sono trattati dal settore privato e dalla maggior parte del settore pubblico**. Il trattamento dei dati da parte delle autorità competenti ai fini dell'applicazione della legge è invece soggetto alla direttiva sulla protezione dei dati nelle attività di polizia e in quelle giudiziarie. Il regolamento generale sulla protezione dei dati **consente alle persone di avere un maggiore controllo sui loro dati personali**, in quanto modernizza e unifica le norme che consentono alle aziende di ridurre la burocrazia e di godere di una maggiore fiducia da parte dei consumatori. Allo stesso tempo, il Gdpr istituisce un sistema di autorità di controllo completamente indipendenti incaricate di monitorare e garantire il rispetto delle norme. Per quanto riguarda i **diritti delle persone**, il Gdpr rafforza i diritti esistenti, prevede nuovi diritti e dà alle persone un maggiore controllo sui loro dati personali. Nello specifico, il Gdpr prevede un migliore accesso ai propri dati, compresa la fornitura di maggiori informazioni su come i dati vengono trattati e la garanzia che tali informazioni siano chiare e comprensibili. Inoltre, il Gdpr prevede un nuovo **diritto alla portabilità dei dati**, che agevola la trasmissione dei dati personali tra prestatori di servizi, un più chiaro **diritto alla cancellazione**, il cosiddetto diritto all'oblio, per cui quando un soggetto non vuole più che i suoi dati vengano trattati e non vi è alcuna ragione legittima per conservarli, i dati saranno cancellati. Infine, il Gdpr prevede il **diritto di sapere se i propri dati personali sono stati violati**, per cui le aziende e le organizzazioni sono tenute a informare l'autorità di controllo competente in materia di protezione dei dati e, in caso di violazione dei dati grave, anche gli interessati. Per quanto concerne le **regole per le imprese**, il Gdpr crea condizioni di parità per tutte le aziende che operano nel mercato interno dell'Ue, adotta un approccio neutrale dal punto di vista tecnologico e stimola l'innovazione attraverso una serie di passi, tra cui un unico complesso di norme a livello europeo: in tal modo, una sola legge per la protezione dei dati a livello europeo rafforza la **certezza del diritto** e **riduce gli oneri amministrativi**. Il Gdpr prevede che le autorità pubbliche e le imprese che trattano dati su larga scala o la cui attività principale è il trattamento di categorie speciali di dati, come i dati relativi alla salute, devono designare una persona **responsabile della protezione dei dati**, ma anche uno sportello unico. Questo per far sì che le imprese possano confrontarsi con una sola autorità di controllo nello Stato membro europeo in cui hanno il loro stabilimento principale. Inoltre, le autorità di controllo pertinenti cooperano nel quadro del comitato europeo per la protezione dei dati per i casi transfrontalieri. Invece **le aziende con sede al di fuori dell'Ue devono applicare le stesse norme quando offrono beni o servizi**, o quando monitorano i comportamenti delle persone all'interno dell'Ue. Queste norme favoriscono l'innovazione, poiché sono una garanzia del fatto che la protezione dei dati sia incorporata nei prodotti e nei servizi fin dalle primissime fasi di sviluppo, contemplando la protezione dei dati fin dalla progettazione e per impostazione predefinita. Il Gdpr mira ad avere delle **tecniche rispettose della privacy**. È incoraggiato ad esempio il ricorso alla **pseudonimizzazione** (quando i campi identificativi all'interno di un set di dati sono sostituiti da uno o più identificatori artificiali) e alla **cifratura** (quando i dati sono codificati in modo tale che possano leggerli solo gli utenti autorizzati), al fine di limitare l'invasività del trattamento. Ancora, **il Gdpr ha eliminato la maggior parte degli obblighi di notifica** e i costi ad essi associati: uno degli obiettivi è

quello di rimuovere gli ostacoli che condizionano la libera circolazione dei dati personali all'interno dell'Ue, affinché per le aziende sia più facile espandersi nel mercato unico digitale. Il Gdpr prevede **valutazioni d'impatto sulla protezione dei dati**: le organizzazioni dovranno pertanto effettuare valutazioni d'impatto qualora il trattamento dei dati presentasse un rischio elevato per i diritti e le libertà delle persone. Il Gdpr obbliga le imprese e gli enti alla tenuta dei registri delle attività di trattamento dei dati. Le piccole e medie imprese non sono tenute alla **registrazione delle attività di trattamento dei dati**, a meno che il trattamento sia abituale o possa comportare un rischio per i diritti e le libertà della persona i cui dati sono in fase di elaborazione o riguardi categorie di dati sensibili. Infine, il Gdpr prevede un moderno pacchetto di **strumenti per il trasferimento internazionale dei dati**. Il Gdpr offre vari strumenti per trasferire i dati al di fuori dell'Ue, tra cui le decisioni in materia di adeguatezza adottate dalla Commissione europea laddove il paese terzo offra un adeguato livello di protezione, clausole contrattuali (tipo) pre-approvate, norme vincolanti d'impresa, codici di condotta e certificazione. A distanza di 4 anni, sebbene sia ancora presto per valutare pienamente il funzionamento dei nuovi meccanismi, **le autorità nazionali di protezione dei dati hanno sviluppato la loro cooperazione attraverso il meccanismo dello sportello unico** e un ampio ricorso all'assistenza reciproca. Si ricorre al meccanismo dello sportello unico, che è una risorsa fondamentale del mercato interno, per decidere numerosi casi transfrontalieri. Sono attualmente pendenti importanti decisioni aventi dimensione transfrontaliera che saranno soggette al meccanismo dello sportello unico. Tali decisioni, che coinvolgono spesso società multinazionali tecnologiche di grandi dimensioni, avranno un impatto sostanziale sui diritti delle persone fisiche in numerosi Stati membri. Tuttavia **lo sviluppo di una cultura europea veramente comune in materia di protezione dei dati tra le autorità di protezione dei dati è un processo ancora in corso**. Le autorità di protezione dei dati non si sono ancora pienamente avvalse degli strumenti previsti dal regolamento generale sulla protezione dei dati, quali le operazioni congiunte che potrebbero condurre a indagini congiunte. A volte, la ricerca di un approccio comune ha comportato un avanzamento secondo il denominatore comune più basso e, di conseguenza, non sono state sfruttate le possibilità per promuovere una maggiore armonizzazione. Infine, la Commissione europea riconosce che **sono necessari ulteriori progressi per rendere più efficiente e armonizzata la gestione dei casi transfrontalieri in tutta l'Ue**, anche sotto il profilo procedurale, ad esempio in merito a questioni quali le procedure di trattamento dei reclami, i criteri di ammissibilità per i reclami, la durata dei procedimenti dovuti a scadenze diverse o all'assenza di termini nel diritto processuale amministrativo nazionale, il momento della procedura in cui è concesso il diritto di essere ascoltati o di informazione e la partecipazione, durante il procedimento, di coloro che presentano il reclamo. —

Sostieni l'informazione libera di Città Nuova! Come? [Scopri le nostre riviste, i corsi di formazione agile](#) e [i nostri progetti](#). Insieme possiamo fare la differenza! Per informazioni: rete@cittanuova.it