Regolamento europeo in materia di protezione dei dati personali

FormezPA

Questo materiale didattico è stato realizzato da Formez PA nell'ambito del Progetto OpenRAS, in convenzione con la Regione Sardegna.

Il Progetto OpenRAS è finanziato dal POR FSE 2014-2020 (Decisione C 2014 N 10096 del 17/12/2014), Asse 4 - Capacità istituzionale e amministrativa, a valere sull'azione 11.1.1 "Interventi mirati allo sviluppo delle competenze per assicurare qualità, accessibilità, fruibilità, rilascio, riutilizzabilità dei dati pubblici".

Autore: Gianfranco Andriola

Creatore: Formez PA

Data: Ottobre 2017

Regolamento europeo in materia di protezione dei dati personali

Da sempre la pubblica amministrazione raccoglie e cataloga informazioni sui propri utenti questa in forma fanno parte del patrimonio informativo della pubblica amministrazione sono utili in alcuni casi ad erogare i servizi ai cittadini, in altri casi accade che la stessa raccolta e in alcuni casi ancora la certificazione di queste informazioni coincida col servizio stesso basti pensare ad esempio al modo in cui la pubblica amministrazione certifica l'identità o al modo in cui questi dati sono indispensabili per esercitare i propri diritti ad esempio il diritto di voto e la connessione tra la possibilità del voto è la certificazione dell'identità; questo compito nel tempo come è ovvio che sia si evolve e in particolare nell'ultimo periodo ha avuto una forte evoluzione dovuta alle nuove tecnologie; le nuove tecnologie hanno cambiato in maniera radicale il modo in cui la pubblica amministrazione raccoglie le informazioni dei propri utenti e le archivia, basti pensare a tutti i servizi online che la pubblica amministrazione gestisce e che eroga e che quindi hanno bisogno per funzionare delle informazioni personali degli utenti oppure basta pensare al servizio Spid, il servizio di certificazione dell'identità digitale che da qualche anno è attiva in Italia e permette a tutti i cittadini di accedere con un'unica password a tutti i servizi della pubblica amministrazione.

La pubblica amministrazione quindi gestisce, archivia e in alcuni casi certifica le informazioni personali degli utenti. Per informazioni personali facciamo riferimento a tutte quelle informazioni che ci permettono di identificare una persona e ci permettono di conoscere i suoi orientamenti, i suoi stili di vita, il suo stato di salute, qualunque informazione che ci permetta di individuare una singola persona e di avere informazioni sul modo in cui conduce la propria esistenza.

A loro volta le informazioni personali possono avere a seconda di come le guardiamo a seconda delle informazioni che trattano ulteriori definizioni parliamo appunto di dati identificativi nel momento in cui guardiamo informazioni che ci permettono di individuare in maniera puntuale una persona il suo nome il suo cognome, l'immagine del suo volto.

Parliamo invece di dati sensibili nel momento in cui facciamo riferimento a informazioni che ci permettono individuare il suo stile di vita e la sua origine razziale, la sua provenienza etnica il suo credo politico qualunque informazione ulteriore rispetto al modo in cui quell'individuo conduce la propria esistenza.

Infine parliamo di dati giudiziari quando facciamo riferimento a dati che ci permettono di rivelare esistenza determinati provvedimenti giudiziari nei confronti di un soggetto.

Le nuove tecnologie hanno cambiato in maniera radicale il modo in cui la pubblica amministrazione gestisce queste informazioni: da un lato la gestione elettronica, la gestione informatizzata di grande quantità di informazioni personali abilita a tutta una serie di servizi che prima erano praticamente impossibili; dell'altro pome un serissimo problema di sicurezza dei dati e un problema di privacy degli utenti.

Il quadro diventa ulteriormente complesso se si pensa al fatto che la pubblica amministrazione non è l'unico soggetto che gestisce queste informazioni ma da quando c'è internet, da quando in particolare c'è il cosiddetto Web 2.0 e i social media, questa situazione è diventata ulteriormente complessa proprio perché una serie di soggetti esterni alla pubblica amministrazione gestiscono una immensa quantità di dati degli utenti e quindi si pone un problema di trasparenza, un problema di accountability, un problema di privacy, un problema di come queste informazioni vengono regolate per cercare da un lato di offrire quanti più servizi innovativi agli utenti, dall'altro di tutelare i propri diritti anche on line.

Il tracciamento e la persistenza dei dati personali degli utenti è un fenomeno che è destinato a diventare sempre più grande in questo senso si può pensare ad esempio al modo in cui ascoltiamo musica adesso e al modo in cui lo facevamo fino a qualche anno fa: fino alla metà degli anni 90 infatti gli ascolti erano assolutamente analogici ed erano vincolati al momento in cui avvenivano su qualunque piattaforma di riproduzione ad esempio un walkman piuttosto che un giradischi, era una cosa che restava vincolata in quel momento e non produceva una traccia; successivamente con l'arrivo dei file mp3 si è iniziato ad avere un tracciamento ogni volta che un file mp3 veniva riprodotto su un iPod piuttosto che sullo stesso computer lasciava una traccia su quel device però quella traccia restava in possesso del singolo utente che l'aveva riprodotta.

Da qualche anno a questa parte invece c'è il cosiddetto fenomeno della musica in streaming cioè l'utilizzo di piattaforme come Spotify, Deezer o lo stesso Youtube che permettono agli utenti di ascoltare musica non caricata sulla propria memoria fisica, sul proprio computer piuttosto che sul proprio smartphone e quindi ogni volta che qualunque utente ascolta un pezzo questo pezzo produce un trattamento, questo ascolto produce dei dati che non restano di proprietà degli utenti ma sono di proprietà del servizio che offre musica in streaming.

Questo esempio ci lascia capire come sempre più i gesti che fino a qualche anno fa erano

analogici e non producevano un tracciamento una persistenza dei dati da qualche anno a questa parte continuano a produrre dati.

Questo stesso discorso può essere esteso a tutta una serie di gesti che compiamo quotidianamente ogni volta ad esempio che ci spostiamo con uno smartphone in tasca che ha il rilevatore GPS acceso stiamo producendo dei dati sul modo in cui ci muoviamo nello spazio; ogni volta ad esempio che navighiamo su internet e ci spostiamo tra i vari siti, quei siti al loro interno hanno una serie di tecnologie che solitamente vengono chiamate cookie, che tracciano il nostro comportamento e aiutano i gestori di siti web ad orientare la loro offerta a seconda di come gli utenti utilizzano quel servizio; questo discorso diventa sempre più ampio dal momento in cui ad esempio pensiamo alle cosiddette tecnologie indossabili, gli smartphone che iniziano ad essere sempre più diffusi, tracciano una serie di attività biometriche dei singoli utenti e quindi ancora una volta producono una quantità di dati sui singoli soggetti, dati sensibili, dati che ci aiutano a tracciare il suo stile di vita, dati che ci aiutano a capire come quell'utente si sta comportando in quel momento.

Questo fenomeno è chiamato “internet of things” cioè il fatto che gli oggetti siano connessi tra di loro e che il modo in cui dialogano l'un l'altro passi attraverso internet, passi attraverso una connessione. Questo fenomeno non va visto necessariamente in accezione negativa al contrario la possibilità di connettere oggetti tra di loro offre per la prima volta servizi che fino a qualche tempo fa erano inimmaginabili però pone un serissimo problema di privacy, pone un problema di sicurezza, pone certamente un problema di sicurezza informatica ma anche un problema di conoscenza, di capacità degli utenti di misurarsi con un fenomeno così complesso e certamente pone un problema di accountability; il modo in cui queste informazioni vengono gestite è essenziale per regolarne il mercato e quindi è importante che la pubblica amministrazione è importante che la politica è importante che qualunque soggetto che ha la possibilità di farlo possa regolare il mercato possa definire le regole del gioco in maniera tale che da un lato portino vantaggi in termini servizi agli utenti però dall'altro questi vantaggi vengano bilanciati da una consistente preservazione della privacy di ogni singolo utente.

Da un punto di vista normativo in Italia il trattamento dei dati personali degli utenti è trattato in maniera organica sin dal 2003 col cosiddetto Codice della Privacy, ora codice in materia di protezione dati personali, che definisce tutta una serie di provvedimenti una serie di diritti dei singoli cittadini nel momento in cui esiste un soggetto che archivia i loro dati e dall'altro pone tutta una serie di obblighi da parte dei soggetti a cui devono attenersi tutti i soggetti che gestiscono i dati personali degli utenti.

La normativa nazionale in materia di conservazione e trattamento dei dati personali degli utenti viene rilanciata a livello europeo con un provvedimento assolutamente importante che è destinato a cambiare il modo in cui pensiamo e organizziamo la privacy dei dati dei singoli utenti e cioè il regolamento europeo in materia di protezione dati personali che ha concluso il suo iter legislativo nel 2016 e aveva piena applicazione in tutti i paesi dell'unione europea il 25 maggio del 2018.

Il regolamento europeo è nato per rispondere a precise esigenze che fino a qualche anno fa non erano avvertite proprio perché il fenomeno della diffusione di internet del modo in cui gli utili gli utenti utilizzano in maniera così massiva la rete ancora non era avvenuto però continuando negli anni la gestione dei dati personali diventa sempre più centrale e quindi l'unione europea ha deciso come dire di mettere mano a questa materia in maniera organica rispondendo ad alcune esigenze precise; innanzitutto semplificare le informazioni sul trattamento dei dati personali degli utenti dal momento in cui sottoscriviamo un qualunque servizio online, specifichiamo una serie di requisiti che il gestore di questo servizio ci pone e quindi spesso sono difficili da interpretare, è molto complesso per gli utenti capire che cosa significa quindi la normativa europea impone per i gestori dei servizi on line la semplificazione di questo scambio, di questa sorta di contratto tra utente e gestione del servizio.

Altra esigenza a cui il regolamento europeo risponde è la cosiddetta garanzia del diritto all'oblio cioè la possibilità di un utente di vedere cancellati propri dati personali presso qualunque soggetto esterno che li gestisce è importante nel momento in cui pensiamo che questi servizi a lungo andare e in termini temporali molto ampli archiviano la vita degli utenti quindi è giusto è responsabile è fonte di accountability il fatto che qualunque utente in qualunque momento possa decidere rispettando ovviamente i termini di servizio di vedere i propri dati cancellati dalle piattaforme che le ospitano.

La portabilità dei dati degli utenti è un altro dei principi a cui il regolamento europeo vuole rispondere e cioè la possibilità di un qualunque utente che ha sottoscritto un servizio con un operatore, di spostare i propri dati da qualche altra parte, basti pensare ad esempio le caselle di posta elettronica e al modo in cui un utente può decidere di rivolgersi a un altro servizio e quindi deve essere messo nelle condizioni di poter estrarre la propria cronologia di posta elettronica dal servizio e che utilizzava per rivolgersi a qualcun altro.

È un discorso più o meno simile se pensiamo ad esempio con la musica fatto prima anche in quel caso se volessimo cambiare la piattaforma in gestione della nostra musica dovremmo

poterci rivolgere a qualcun altro avendo la possibilità di esportare i nostri dati e quindi riversarli magari su una nuova piattaforma che pone delle condizioni di mercato più vantaggiose.

Questo fenomeno di solito viene chiamato come data lock-in cioè alcune piattaforme per proprio interesse economico tendono a rendere difficile l'esportazione dei dati degli utenti proprio per legarle in maniera ulteriore la normativa europea da un'espressione su questo atteggiamento di alcuni gestori di servizi online e quindi rafforza la posizione degli utenti nei confronti di gestori dei servizi.

Altro obiettivo che il regolamento europeo in materia di protezione dei dati personali si pone è la cosiddetta armonizzazione delle norme per tutti gli stati dell'unione europea, anche qui è un fenomeno che fino a un po' di tempo fa, fino a che internet diventasse così organica così pervasiva quasi non se ne sentiva l'esigenza però in questo momento cioè nel momento in cui qualunque utente può sottoscrivere un servizio online caricato su un server che si trova in qualunque paese del mondo, avere l'armonizzazione delle norme che tutelano gli utenti all'interno del modo in cui questi utenti interagiscono con i vari servizi è assolutamente centrale e quindi è un punto centrale, un punto di assoluta rilevanza affrontato dal regolamento europeo in materia di protezione dei dati personali.

Abbiamo appena visto le esigenze a cui il regolamento europeo vuole rispondere, proviamo a vedere i principi attraverso cui il regolamento europeo opera.

Il primo principio, quello messo in assoluto risalto dal regolamento europeo in materia di protezione dei dati personali è il principio dell'accountability cioè la piena responsabilizzazione del gestore dei dati nei confronti dei singoli utenti; è importante che il gestore abbia consapevolezza di quanto rilevanti siano queste informazioni e quindi adotti tutte le misure necessarie a renderla quanto più sicure possibili.

Secondo principio attraverso cui la normativa europea guarda alla tutela del trattamento dei dati personali è la cosiddetta privacy by design cioè la possibilità che nel momento in cui si progetta, si sviluppa un servizio online gestirà dati degli utenti sia innanzitutto garantita la protezione dei dati degli utenti stessi cioè degli utenti che andranno a utilizzare quel servizio e non è solo un principio è estremamente operativa la cosiddetta privacy by design cioè la possibilità che all'interno di un'organizzazione che gestisce dati degli utenti vengono individuate delle figure chiave nell'organico organizzativo che gestiscono tutti i vari passaggi che tutelano la privacy degli utenti e vengano fatte tutta una serie di prove di test sui servizi che devono andare online in maniera tale che ancora una volta la privacy degli utenti venga

messa al centro, la protezione di dati personali venga messa al centro della progettazione del servizio stesso.

Altro principio che poi diventa estremamente operativo nella pratica amministrativa, nel modo in cui il regolamento europeo andrà a impattare sul modo in cui sia i soggetti privati che i soggetti pubblici gestiscono i dati degli utenti sono le sanzioni amministrative; il regolamento prevede risoluzioni amministrazioni estremamente salate riconosciute fino a 10 milioni di euro e questa cosa ci dà la dimensione di quanto l'unione europea tenga, di quanto l'unione europea voglia utilizzare in maniera estremamente puntuale, in maniera estremamente consistente, il regolamento europeo in materia di dati personali per tutelare la privacy degli utenti dei cittadini europei.

Come già detto, il regolamento europeo in materia di protezione dei dati personali si applica sia alle imprese private che agli enti pubblici diventerà pienamente operativo nel maggio 2018 e fino ad allora le pubbliche amministrazioni possano iniziare ad organizzarsi implementando all'interno delle singole organizzazioni tutta una serie di misure volte a farsi trovare preparate dal momento in cui il regolamento europeo diventa pienamente operativo anche nella norma italiana.

La prima misura da adottare per le pubbliche amministrazioni che appunto vogliono farsi trovare preparate nel momento in cui il regolamento europeo diventerà pienamente operativo è la nomina del responsabile della protezione dei dati personali è una figura cardine una figura centrale nel momento in cui le pubbliche amministrazioni vogliono far diventare operativi principi e le indicazioni date dal regolamento europeo; è la figura che porta alla responsabilizzazione appunto l'accountability delle amministrazioni nei confronti degli utenti quando si parla di trattamento dei dati personali.

Nel momento in cui un ente pubblico opera una nomina del responsabile della protezione dei dati personali deve tenere presenti alcuni principi che portano appunto a individuare la persona giusta il riferimento giusto all'interno dell'ente: il principio di posizione (cioè è una figura che riferisce direttamente al vertice dell'organizzazione), il principio di indipendenza e il principio di autonomia (cioè ed adesso una figura dotata di un proprio budget in maniera tale che possa fare scelte indipendenti da quelle che sono le indicazioni delle amministrazioni e operare quindi nel pieno interesse degli utenti che devono vedere i propri dati e le proprie informazioni personali tutelate dall'ente pubblico).

Seconda azione da mettere in campo per le pubbliche amministrazioni che vogliono appunto

farsi trovare preparate nel momento in cui il regolamento europeo diventerà operativo è il registro delle attività del trattamento: sostanzialmente si tratta di una cernita di tutte le banche dati già detenute dagli enti che hanno al loro interno dati personali e dati sensibili degli utenti quindi capire quali sono questi dati capire dove sono e organizzarsi in maniera da poterli trattare al meglio.

Terza azione del poter fare sin da subito è la notifica delle violazioni dei dati personali è sempre più frequente si sente sempre più spesso anche sui giornali o su internet che soggetti esterni molto spesso malevoli intervengono violano le banche dati delle pubbliche amministrazioni ma anche delle aziende private rubando di fatto i dati degli utenti in questo caso, qualunque ente pubblico potrà organizzarsi in questo senso provando a ragionare su quali sono le notifiche delle violazioni dei dati e come poter intervenire nel caso in cui malauguratamente un episodio di questo tipo si dovesse verificare al momento in cui ci dovesse essere un furto dei dati personali come una pubblica amministrazione può reagire come può notificare questo furto, l'avvenuto furto gli utenti e come può attivare delle misure per fare in modo che questi episodi non si verifichino più.

Per l'Italia la figura di riferimento rispetto al modo in cui viene attuato nel nostro paese il regolamento europeo in maniera di protezione di dati personali è certamente il Garante per la protezione dei dati personali italiano che fra l'altro ha attivato sul proprio sito una sezione dedicata al regolamento europeo costantemente aggiornate e piena di spunti operativi sia per enti privati che per pubbliche amministrazioni che vogliono farsi trovare preparate al momento in cui il regolamento europeo diventerà pienamente operativo anche in Italia.