Matricola n. 0000933896

ALMA MATER STUDIORUM

UNIVERSITA' DI BOLOGNA

SCUOLA DI SCIENZE

CORSO DI LAUREA TRIENNALE IN INFORMATICA PER IL MANAGEMENT

ADEMPIMENTI ED OBBLIGHI CHE OGNI APP DEVE RISPETTARE

Tesi di laurea in DIRITTO DI INTERNET

Relatore

Prof.ssa Matilde Ratti

Presentata da

Lucrezia Ilvento

Sessione terza

Anno Accademico 2021/2022

INDICE

INTRODUZIONE

Il tema della privacy e della protezione dei dati personali è diventato sempre più rilevante negli ultimi anni, grazie alla crescente diffusione della tecnologia e della digitalizzazione. In particolare, l'entrata in vigore del GDPR, il Regolamento Europeo per la protezione dei dati personali, ha avuto un impatto significativo sulla gestione dei dati personali da parte delle aziende e degli individui.

In questa tesi si esaminerà il ruolo del GDPR nella protezione dei dati personali, con particolare attenzione alla sua applicazione nello sviluppo di un'applicazione. Inoltre, si analizzerà l'emergenza sanitaria del COVID-19 e il ruolo dell'app Immuni nel rispetto della privacy e nella protezione dei dati personali.

Il primo capitolo sarà dedicato alla descrizione del GDPR e delle sue definizioni fondamentali, nonché dei principi applicabili al trattamento dei dati personali.

Nel secondo capitolo, si analizzerà il processo di sviluppo di un App e le leggi applicabili alla protezione dei diritti di proprietà intellettuale e sulla concorrenza e il mercato.

Infine, il terzo capitolo si concentrerà sull'emergenza sanitaria del COVID-19 e l'utilizzo dell'app Immuni, esaminando le implicazioni per la privacy e la protezione dei dati personali.

In conclusione, questa tesi evidenzierà l'importanza del rispetto della privacy e della protezione dei dati personali nella società digitale attuale e come il GDPR possa contribuire a garantirli.

CAPITOLO 1

GDPR: UN REGOLAMENTO EUROPERO PER LA PROTEZIONE DEI DATI PERSONALI

Sommario: 1. Il diritto alla protezione dei dati personali. Le definizioni fondamentali - 1.1. Dato personale e dato anonimo – 1.2. I dati sanitari quali dati particolari ai sensi dell'art.9 del GDPR - 1.3. Trattamento dei dati personali – 2. I soggetti del trattamento dei dati personali – 2.1. L'interessato – 2.2. – Il titolare del trattamento – 2.3. Il responsabile del trattamento – 2.4. – Il Data Protection Officer – 3.I principi applicabili al trattamento dei dati personali – 3.1. Il principio di liceità, correttezza – 3.2. Il principio di finalità – 3.3. Il principio di minimizzazione dei dati – 3.4. Il principio di esattezza – 3.5. Il principio di limitazione della conservazione – 3.6. Il principio di integrità e riservatezza – 3.7. Il principio di accountability - 4. Le condizioni di liceità del trattamento.

1. Il diritto alla protezione dei dati personali. Le definizioni fondamentali

Il diritto alla protezione dei dati personali consiste nel diritto di ognuno di esercitare un controllo sui propri dati ove per controllo si intende anche accesso e rettifica degli stessi. Il diritto alla protezione dei dati personali è riconosciuto dalla Carta dei diritti fondamentali dell'Unione europea[1]. L'art.8 della Carta afferma che ogni individuo ha il diritto alla protezione dei dati di carattere personale che lo riguardano. Nel secondo punto dell'articolo si dice che tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge e che ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Sempre nell'art.8 si afferma che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.
Il diritto alla protezione dei dati personali si configura, dunque, come il diritto di un soggetto di controllare l'insieme delle informazioni che allo stesso si riferiscono e che quindi costituiscono il suo riflesso e delineano lo stesso suo essere nella società dell'informazione.[2]
L'art.7 della Carta dei diritti fondamentali dell'Unione europea afferma il diritto al rispetto della vita privata e familiare, del proprio domicilio e delle sue comunicazioni. Quest'articolo riconosce il diritto alla riservatezza che va distinto dal diritto alla protezione dei dati personali. Il diritto alla riservatezza è da intendersi come libertà negativa di non subire interferenze nella propria vita privata. Il diritto alla protezione dei dati personali, invece, costituisce il fondamento della libertà positiva di esercitare un

[1] La Carta dei diritti fondamentali dell'Unione europea è stata approvata il 7 dicembre 2000 e contiene gli ideali su cui si fonda l'Unione europea.

[2] Cfr. RODOTA', *Tecnologie e diritti*, Bologna ,1995, p.11.

controllo sul flusso delle proprie informazioni. Il diritto alla protezione dei dati personali rientra tra i diritti della personalità ossia quella categoria aperta di diritti caratterizzati dall'essere assoluti, indisponibili e imprescrittibili.
L'evoluzione tecnologica ha aperto un dibattito culturale in merito alla protezione dei dati personali. Dietro ciò un lungo percorso normativo che ha avuto inizio con la "Direttiva madre" in materia di protezione di dati personali, la Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. La Direttiva è stata poi sostituita dal "Codice in materia di protezione dei dati personali[3]"[3]. Un'ulteriore tappa di questo percorso è segnata dal Regolamento europeo 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali applicabile dal 25 maggio 2018. Il Regolamento generale sulla protezione dei dati conosciuto anche come GDPR (dall'inglese *General Data Protection Regulation*)è un regolamento europeo che disciplina il modo in cui le aziende e le altre organizzazioni trattano i dati personali. Questo nasce come strumento per uniformare il diritto per gli Stati europei, infatti, trattandosi di regolamento, esso è direttamente applicabile in tutti gli Stati membri dell'Unione Europea senza la necessità di ulteriori norme a livello nazionale. La legge mira a proteggere "i diritti e le libertà fondamentali delle persone fisiche " dando a ciascuna persona il controllo su come vengono utilizzati i propri dati personali. A tal fine, stabilisce requisiti rigorosi e precisi per il trattamento dei dati, nonché per la trasparenza, la produzione, l'archiviazione della relativa documentazione e consenso dell'utente.

1.1 Dato personale e dato anonimo

Dato personale è una qualsiasi informazione relativa a una persona fisica, giuridica, ente o associazione indentificata o identificabile. Una persona fisica è considerata identificabile se può essere identificata, direttamente o indirettamente, da una o più caratteristiche identificative come il nome, il numero di identificazioni, l'ubicazione o l'identificativo online[44].

Il dato personale è, quindi, qualunque informazione riferibile a qualunque soggetto.

Il dato personale non è necessariamente un dato riservato ma può essere anche un dato noto a più persone come un numero di cellulare o un indirizzo di posta elettronica.

Il dato può essere collegato all'interessato in via diretta ma anche in via indiretta o mediana attraverso un codice.

Dato anonimo, invece, è quel dato che, in origine o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.[5]

L'anonimato è un concetto relativo in quanto un'informazione può essere anonima per una persona e non esserlo per un'altra.

La ragionevolezza diviene quindi il criterio di valutazione della collegabilità e della riconducibilità delle informazioni al fine di distinguere i dati anonimi da quelli riconducibili a soggetti.

[3] D.lgs. 30 giugno 2003, n.196.

[4] Art.4 GDPR.

[5] Considerando n.26 GDPR.

1.2 I dati sanitari quali dati particolari ai sensi dell'art.9 del GDPR

L'art.4 del Reg. UE n.2016/679 indica come dati sanitari quei dati relativi alla salute; si intende i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

L'articolo 9 del GDPR stabilisce che i dati particolari non possono essere trattati salvo che vi sia il consenso esplicito dell'interessato o in caso di necessità per assolvere ad alcuni obblighi di legge ben codificati all'interno della norma medesima.

Dalla lettura del primo paragrafo dell'art.9 è possibile comprendere quali siano le tipologie di dati considerate particolari secondo il regolamento e, segnatamente, quei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, biometrici e quelli relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il paragrafo 2 dello stesso articolo prevede però alcuni casi (tassativi) al ricorrere dei quali è possibile derogare al divieto di trattamento genericamente previsto per queste categorie di dati, ossia per eseguire il trattamento dei dati personali nel settore del diritto del lavoro e della protezione sociale, comprese le pensioni, e per finalità di sicurezza sanitaria, controllo e allerta, nonché per la prevenzione o il controllo di malattie trasmissibili e altre minacce gravi alla salute o se il trattamento è necessario per ragioni di interesse pubblico.

Si tratta comunque di un trattamento molto particolare, che deve essere eseguito applicando un complesso quadro regolatorio, composto da principi e regole del GDPR, norme del Codice della privacy novellato e prescrizioni del Garante italiano.

1.3 Trattamento dei dati personali

Trattamento è definito come "qualsiasi operazione o insieme di operazioni , compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione,l'adattamento o la modifica, l'estrazione, la consultazione, l'uso , la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione , il raffronto o l'interconnessione , la limitazione, la cancellazione o la distruzione"[6]. La definizione è particolarmente ampia e include qualsiasi attività compiuta sui dati personali: dalla raccolta, alla condivisione, fino alla cancellazione. Anche l'anonimizzazione, ossia il processo tramite il quale i dati sono resi non più direttamente riferibili ad un singolo individuo, rientra perciò nella categoria di "trattamento". Il GDPR è neutrale sotto il profilo tecnologico, dunque la definizione di trattamento non è legata all'utilizzo di una particolare tecnica o tecnologia. Le operazioni di trattamento, infatti, possono essere interamente automatizzate, ossia compiute attraverso mezzi tecnici in grado di raccogliere e processare le informazioni in maniera autonoma e automatica, o solo parzialmente automatizzate, quindi che richiedono in un certo momento un intervento umano. Quando il trattamento è effettuato manualmente, il GDPR trova applicazione solo nei confronti di insiemi strutturati di dati personali accessibili secondo criteri determinati, indipendentemente dalle modalità di conservazione[7].

[6] Art.2, 1°comma, GDPR.

[7] Cfr. *Privacy e data Protection* 2022, Giulio Coraggio, IPSOA, Milano, p.4.

2. I soggetti del trattamento dei dati personali

Secondo il regolamento, i principali soggetti della protezione dei dati personali sono: l'interessato, il titolare del trattamento dei dati e il Responsabile del trattamento.

2.1 L'interessato

Con l'espressione interessato deve intendersi la persona fisica, identificata o identificabile, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali. Si definisce, dunque, interessato la persona fisica o giuridica, anche se non riconosciuta, i cui dati personali sono oggetto di trattamento.[8]

L'art.4 specifica che si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente mediante un identificativo e fornisce un elenco esemplificativo degli stessi.

La figura dell'interessato, pur rappresentando il lato passivo del trattamento, assume anche un ruolo attivo, dal momento che la normativa sulla protezione dei dati personali riconosce all'interessato una serie di diritti esercitabili nei confronti del titolare del trattamento quali efficaci strumenti di tutela dei propri dati.

2.2 Il titolare del trattamento

Il Codice in materia di protezione dei dati personali considera titolare del trattamento la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione ed organismo, cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza[9].

Tale figura, è inquadrabile come quel soggetto che individua e stabilisce il "perché" e il "come" di certe attività di trattamento [10]e che il Legislatore ha riconosciuto come centro di imputazione giuridica quando il trattamento dei dati viene effettuato per finalità proprie.

Non è prevista la formalizzazione della titolarità[11]. Se il titolare è una persona giuridica, tale è da considerarsi l'ente nel suo complesso. Nel caso di grandi enti o amministrazioni, articolati in direzioni generali o in sedi centrali o periferiche dotate di poteri decisionali del tutto autonomi sui trattamenti effettuati nel loro ambito, le stesse articolazioni possono a loro volta essere considerate come titolati o contitolari del trattamento.[12]

Il trattamento può essere comune a più soggetti che condividono le decisioni circa i mezzi e le finalità del trattamento. Si parla in questi casi di contitolarità del trattamento[13].

Ogniqualvolta che, invece, più soggetti esercitano un potere decisionale del tutto autonomo sui dati personali, a ciascuno di essi dovrà essere imputata la titolarità autonoma

[8] Art.4, GDPR.

[9] Art.4, 1°comma, n.7 del Regolamento.

[10] Cfr. Gruppo di lavoro *ex*.art.29, Parere 1/2010.

[11] Il Regolamento specifica che nel caso in cui le finalità e i mezzi di trattamento siano determinate dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri di designazione dello stessopossono essere stabiliti dal diritto dell'Unione o degli Stati membri.

[12] Cfr. Garante per la protezione dei dati personali, provvedimento del 9 dicembre 1997, in *https//garanteprivacy.it/docweb/30915*.

[13] Art.26 del GDPR.

del trattamento.

2.3 Il responsabile del trattamento

Il responsabile del trattamento è definito come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"[14]. Il suo potere di azione è limitato a operazioni di carattere tecnico-professionale.

Oltre a fornire la definizione del responsabile del trattamento, il Regolamento disciplina anche le modalità e le caratteristiche della designazione[15]. Il responsabile è designato dal titolare facoltativamente ed è possibile procedere alla designazione di più soggetti quali responsabili ("sub-responsabili")[16], se necessario per soddisfare esigenze organizzative.

Inoltre, sia il responsabile che il titolare del trattamento possono individuare persone fisiche che agiscano sotto la loro autorità secondo le istruzioni da loro impartite.

2.4 Il Data Protection Officer

Il Data Protection Officer (DPO) è una figura introdotta dal nuovo Regolamento europeo in materia di protezione di dati personali[17].Il DPO è in realtà l'evoluzione del "privacy officer", figura prevista dalla direttiva europea 95/46 laddove consentiva agli Stati dell'Unione di prevedere semplificazioni o esenzioni nei casi di designazione di un soggetto indipendente che garantisca la corretta applicazione della normativa. Il DPO è un consulente esperto che va ad affiancare il titolare nella gestione delle problematiche del trattamento dei dati personali, in tal modo garantendo che un soggetto qualificato si occupi della materia, aggiornandosi sui rischi e le misure di sicurezza, in considerazione della crescente importanza e complessità del settore. Il DPO è quindi un soggetto che riferisce direttamente al responsabile o titolare del trattamento, ma è dotato di autonomia e di indipendenza. Il titolare e il responsabile del trattamento devono valutare il soggetto da nominare secondo alcuni specifici criteri, come il possesso di un'approfondita conoscenza della normativa e delle prassi in materia di protezione dei dati personali, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.

3. I principi applicabili al trattamento dei dati personali

I principi applicabili al trattamento sono elencati all'art.5, Reg. UE 2016/679 e costituiscono l'architrave della normativa in materia di protezione dei dati personali. Essi rivestono una duplice natura: stabiliscono la norma applicabile nel caso concreto e al contempo fungono da principi-guida per l'interpretazione e l'applicazione dell'intero plesso normativo. In virtù del carattere di neutralità tecnologica della normativa[18], i principi applicabili al trattamento devono essere interpretati in ottica evolutiva, calandoli nella realtà fattuale a seconda degli sviluppi rilevanti, non solo in termini di strumenti e finalità del trattamento, ma anche di contesto storico-tecnologico generale.

[14] Art.4, 1°comma, n.8 del Regolamento.
[15] Art.28 del Regolamento.
[16] La nomina del sub-responsabile è subordinata all'autorizzazione scritta del titolare del trattamento. Quest''ultimo è legato al titolare tramite un contratto e conserva nei confronti del titolare del trattamento l'intera responsabilità di eventuali inadempimenti o violazioni della normativa.
[17] Art.37 del Regolamento.
[18] Considerando n.15 GDPR.

Il titolare del trattamento è tenuto a rispettare i principi applicabili al trattamento e deve essere in grado di dimostrarlo secondo i canoni della responsabilizzazione o "accountability". Eventuali violazioni sono soggette a sanzioni amministrative fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore[19].

Le modalità dei trattamenti e i requisiti dei dati possono quindi essere sintetizzate nei principi di liceità e correttezza del trattamento, di necessità del trattamento, di finalità del trattamento, di esattezza dei dati trattati, di pertinenza e non eccedenza dei dati rispetto alle finalità della raccolta, nonché in quelli relativi all'aggiornamento e alla completezza dei dati trattati.

3.1 Il principio di liceità, correttezza

Un trattamento è lecito solo nella misura in cui si fondi sul consenso dell'interessato ovvero su una base giuridica legittima[20]. Secondo l'art.6 GDPR sono basi giuridiche idonee a fondare il trattamento dei dati personali il consenso dell'interessato, l'adempimento di obblighi contrattuali, la tutela di interessi vitali della persona interessata o di terzi, l'adempimento di obblighi di legge cui è soggetto il titolare, il perseguimento di un interesse pubblico o esercizio di pubblici poteri e l'interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati. Nello stabilire la specifica base giuridica per un determinato trattamento, il titolare deve tenere conto delle finalità perseguite con quel trattamento e distinguerla rispetto alle basi giuridiche impiegate per altri eventuali trattamenti svolti. Al venir meno della base giuridica rilevante, il trattamento deve cessare, tranne nel caso in cui il titolare sia in grado di proseguire il trattamento in maniera lecita impiegando un'ulteriore base giuridica. Il trattamento di categorie particolari di dati personali è invece vietato, salvo che sussista almeno una delle condizioni di cui all'art.9, par2, GDPR.

Il principio di liceità costituisce il fulcro della tutela riconosciuta al diritto alla protezione dei dati.

La correttezza del trattamento va letta congiuntamente alla liceità e fa riferimento principalmente alle concrete modalità cui deve essere improntato il rapporto tra titolare del trattamento e interessati. In particolare, i dati personali non devono essere trattati in modo ingiustificatamente pregiudizievole, illegittimamente discriminatorio, inaspettato o fuorviante per gli interessati. Le misure e i presidi volti all'attuazione del principio di correttezza sono strettamente connessi ai diritti e alle libertà degli interessati, specialmente al diritto all'informazione (trasparenza), al diritto di intervenire sul trattamento (accesso, cancellazione, portabilità dei dati, rettifica), al diritto di limitazione del trattamento e al diritto di non essere soggetti a processi decisionali individuali automatizzati e alla non discriminazione degli interessati in tali processi.

In virtù del principio di correttezza, il titolare deve inoltre astenersi da comportamenti generalmente scorretti nel rapporto con l'interessato, tra cui sfruttare vulnerabilità dell'interessato, indurlo a scelte svantaggiose, vincolare in maniera scorretta l'interessato al consumo dei propri servizi, indurre l'interessato in una situazione di ingiusta soggezione, ovvero tentare di trasferire il proprio rischio d'impresa sull'interessato.

3.2 Il principio di finalità

Con l'espressione principio di finalità si intende la rispondenza del trattamento dei dati

[19] Cfr. *Privacy e data Protection* 2022 , Giulio Coraggio, IPSOA, Milano, p.16.
[20] Art.6, par.1 GDPR.

personali a finalità determinate, esplicite e legittime.

Le finalità si considerano determinate quando il perimento di utilizzo dei dati è ben definito dal titolare che è tenuto a verificare gli scopi specifici per i quali intende trattare i dati. Il principio assume rilevanza soprattutto con riguardo alle operazioni di trattamento effettuate da soggetti pubblici, laddove – diversamente da quanto accade per le operazioni di trattamento effettuate da soggetti privati – il presupposto di legittimità non è il consenso dell'interessato bensì la strumentalità delle operazioni di trattamento allo svolgimento delle funzioni istituzionali. Le finalità prefissate dal titolare devono essere determinate e legittime, nonché rese esplicite attraverso diverse misure, fra le quali innanzitutto l'informativa da rendere agli interessati. L'esplicitazione delle finalità è essenziale per l'interessato, in quanto consente a questi di meglio esercitare il controllo sul flusso dei propri dati personali, di manifestare un consenso, ove previsto, libero ed informato, e di esercitare al meglio il diritto alla cancellazione, rettificazione o integrazione dei dati che lo riguardano.

Il livello di dettaglio con cui il titolare è tenuto a fornire informazioni sulle finalità del trattamento dipende dal contesto in cui i dati sono raccolti, dal tipo di dati personali trattati e dalla natura soggettiva degli interessati coinvolti.

Le finalità sono esplicite laddove siano rese manifeste all'esterno della sfera del titolare del trattamento e delineate in modo chiaro e privo di ambiguità nei confronti degli interessati, delle autorità di controllo e degli altri soggetti coinvolti nel trattamento.

3.3 Il principio di minimizzazione dei dati

Il principio di minimizzazione dei dati sostiene che il trattamento di dati personali deve essere effettuato in modo da ridurre al minimo l'uso dei dati personali e di quelli identificativi, al fine di escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere raggiunte mediante rispettivamente dati anonimi o opportune modalità che permettano di identificare l'interessato solo in caso di necessità[21]. Ulteriore regola connessa al principio di minimizzazione è quella di prevedere che le informazioni dell'interessato, digitali e no, siano conservate in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario al raggiungimento degli scopi per i quali sono state raccolte o successivamente trattate. Trascorso questo periodo, i dati devono essere cancellati o trasformati in forma anonima, garantendo così il diritto all'oblio dell'interessato, ovvero il diritto che talune informazioni relative all'interessato siano dimenticate. I dati possono, inoltre, essere raccolti esclusivamente se necessari per le finalità del trattamento e devono essere conservati solo per il periodo di tempo a ciò indispensabile.

3.4 Il principio di esattezza

In base al principio di esattezza [22]i dati personali devono essere "esatti e, se necessario, aggiornati". Ne deriva l'obbligo in capo al titolare del trattamento di adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati. Il trattamento di dati inesatti potrebbe infatti comportare rischi per le libertà e i diritti degli interessati, sia nel caso di impiego di mezzi manuali che

[21] Art.5, 1°comma del GDPR.
[22] Art.5, 1°comma, lett. d) del GDPR.

automatizzati, ovvero di processi decisionali automatizzati come gli strumenti di intelligenza artificiale. Il principio di esattezza è strettamente connesso al diritto degli interessati di ottenere la rettifica dei dati personali inesatti che li riguardano e l'integrazione dei dati personali incompleti.

Il titolare è tenuto a adottare sistemi tecnici e organizzativi che gli consentano di verificare agevolmente e con cadenza regolare l'esattezza dei dati, così come di valutare la necessità di un eventuale aggiornamento, in considerazione delle specifiche finalità del trattamento. Quanto alla configurazione iniziale del trattamento, il titolare dovrebbe preferire sistemi in grado di minimizzare l'inesattezza dei dati. Infine, il titolare deve essere pronto a dare seguito a eventuali richieste legittime di cancellazione o rettifica dei dati nei termini prescritti dalla legge.

3.5 Il principio di limitazione della conservazione

Il principio di limitazione della conservazione impone che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati[23]. Trascorso questo periodo, i dati devono essere cancellati o trasformati in forma anonima. Il periodo di conservazione dei dati è responsabilità del titolare. La normativa vigente dispone, in alcuni casi, sui termini di conservazione.

3.6 Il principio di integrità e riservatezza

Il principio di integrità e riservatezza prevede che i dati devono essere trattati in modo da garantirne un'adeguata sicurezza, compresa la protezione mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. L'adeguata sicurezza dei dati riguarda l'aspetto informatico, giuridico ed organizzativo.

3.7 Il principio di accountability

Il principio di accountability prevede che il titolare del trattamento sia, da un lato, responsabile per il rispetto della normativa applicabile in materia di protezione de dati personali e, dall'altro, in grado di dimostrate attivamente e in concreto la propria conformità.

Il termine accountability può essere tradotto con responsabilità e, insieme, prova della responsabilità.[24]

Il principio di accountability viene citato in molte disposizioni del Regolamento in materia di protezione di dati personali.

Nel Regolamento si prevede che tale principio gravi, in particolare, sul titolare che avrà l'obbligo di rispettare i principi generali del trattamento e, al contempo, sarà tenuto a dimostrare di avere adottato misure di sicurezza adeguate ed efficaci.[25]

L'art.25 par.2, prevede che il titolare debba mettere in atto misure tecniche e organizzative adeguate a garantire che siano trattati per impostazione predefinita, solo i dati personali, necessari per specifica finalità del trattamento. Si determina, inoltre, un controllo che

[23] Art.5, 1°comma, lett. e) del GDPR.

[24] Cfr. Gruppo di lavoro *ex*.art.29, Parere 3/2010.

[25] Cfr. Considerando n.78.

attienealla raccolta, la portata del trattamento, limitazioni al periodo di conservazione e all'accesso.[26]

4. Le condizioni di liceità del trattamento

Affinché il trattamento di dati personali possa considerarsi lecito, è in primo luogo necessario che esso sia fondato su una delle basi giuridiche previste disciplinate dagli artt. 6, 9 e 10 GDPR. In assenza di tali basi giuridiche, il trattamento non può essere effettuato.

Tra le condizioni di liceità del trattamento vi è il consenso dell'interessato[27]. Per consenso s'intende qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento[28].L'interessato deve avere previamente ricevuto alcune informazioni, contenute nella cosiddetta informativa, complete e adeguate, circa il trattamento dei dati, al fine di potere validamente decidere se prestare o meno il proprio consenso. Il consenso, inoltre, deve essere libero. Infine, il consenso deve essere specifico, cioè espresso in relazione ad una determinata finalità di trattamento.

Oltre al consenso, si è già precedentemente rilevato come il Legislatore europeo abbia previsto altri cinque presupposti alternativi, che ugualmente legittimano il trattamento dei dati personali. Partendo dalla lettura della lett. b) dell'art. 6 par. 1 del Regolamento, si evince l'introduzione di una condizione di favore per le relazioni economiche: infatti, nel bilanciamento tra interessi contrapposti, in questo caso, risulta prevalente quello alla circolazione dei dati personali, ammettendosi che il trattamento possa considerarsi legittimo qualora risulti necessario all'esecuzione di un contratto o di trattative precontrattuali richieste dall'interessato.

Terzo presupposto legittimante è l'esecuzione di un obbligo legale, previsto dalle norme dell'Unione Europea o di uno Stato membro, al quale è soggetto il titolare del trattamento.

Proseguendo nella disamina, ulteriore condizione di liceità prevista è quella definibile come trattamento dei dati per stato di necessità.

Il trattamento è lecito, altresì, nella misura in cui sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è incaricato il titolare.

Particolarmente rilevante è, infine, l'ultimo presupposto previsto in chiosa all'elenco del par. 1 dell'art. 6 in esame, individuato nel perseguimento di un legittimo interesse del titolare o di terzi.

Il titolare, inoltre, è tenuto a fornire idoneo atto di informazione all'interessato tramite l'informativa. È richiesto che il titolare del trattamento adotti le misure idonee affinché la stessa venga fornita gratuitamente in forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile, con un linguaggio semplice e chiaro[29], modulato alla luce delle caratteristiche soggettive dell'interessato.

---

[26] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali, il Regolamento europeo2016/679*, Giappichelli Editore, Torino, 2016, p.45.

[27] Soggetto i cui dati vengono trattati.

[28] Art.4, par.11 del Regolamento.

[29] Secondo quanto previsto al Considerando 58, l'uso dei mezzi elettronici risulta particolarmente utile in situazioni caratterizzate da una molteplicità di operatori coinvolti e da operazioni di particolare complessità tecnologica, in cui è più difficile per l'interessato comprendere da chi e per quali finalità avviene il trattamento.

I contenuti dell'informativa sono, invece, tassativamente elencati negli artt. 13 par. 1 e 14 par. 1 del Regolamento, i quali definiscono i dati che devono essere forniti all'interessato quando sono, rispettivamente, raccolti dall'interessato ovvero ottenuti da un'altra fonte.

CAPITOLO 2

SVILUPPO DI UN APP

Sommario: 1. Legge applicabile - 1.1. GDPR e sviluppo di un App – 1.2. Protezione dei diritti di proprietà intellettuale - 1.3. La legge sulla concorrenza e il mercato – 2. Linee guida per la conformità alla normativa –3. Come le tecnologie emergenti stanno influenzando le questioni legali relative allo sviluppo di un App.

1. Legge applicabile

"App" è l'abbreviazione del termine informatico Applicazione. Nello specifico settore "Mobile" per App si intende un'applicazione o un programma creato per essere installato su dispositivi Cellulari o Mobili che interagisce con i componenti del cellulare e con l'utente che lo utilizza. Un'applicazione è un software che si distingue per la semplicità, essenzialità e velocità, adattandosi alle limitate risorse hardware dei dispositivi mobili.[30]

Le App possono essere scaricate dagli app store di cui ciascun sistema operativo dispone.

Il settore delle applicazioni mobili, o "App", è in continua evoluzione e ha portato con sé diverse questioni legali tra gli autori che le progettano. La mancanza di norme di legge specifiche per la figura dell'App e del suo creatore ha portato a controversie nell'ordinamento giuridico. In Italia, per lo sviluppo di un App sono applicabili diverse normative, tra cui il Regolamento Generale sulla Protezione dei Dati (GDPR), la legge sulla proprietà intellettuale e la legge sulla concorrenza e il mercato.

È importante che i produttori di App siano consapevoli delle norme applicabili e seguano le linee guida appropriate per garantire che la loro applicazione sia conforme alle stesse. In particolare, il GDPR impone ai produttori di informare gli utenti su come verranno utilizzati i loro dati personali, richiede che sussista una delle basi giuridiche del trattamento di cui all' art.6 affinché i dati possano essere trattati (qualora questa sia il consenso, impone di, fornire all'utente un modo per revocare il consenso prestato) e che siano previste, misure di sicurezza adeguate per la protezione dei dati raccolti, impone al titolare di notificare le autorità competenti in caso di violazione della sicurezza e disciplina i diritti dell'interessato, tra cui quelli di : consentire l'accesso ai propri dati personali, correggere o, al ricorrere di determinate situazioni, eliminare gli stessi.

[30] Cfr. M. Iaselli ,*I problemi giuridici che scaturiscono dallo sviluppo e dall'utilizzo delle applicazioni ne settore mobile sono fondamentalmente due: quello relativo al trattamento dei dati, ovvero della privacy e quello relativo alla qualificazione giuridica delle App*, Roma ,2015.

La legge sulla proprietà intellettuale, invece, riguarda il riconoscimento e la protezione dei diritti di proprietà intellettuale, come brevetti, marchi, diritti d'autore e segreti commerciali. Il modello giuridico di tutela del software consiste nella protezione quale opera dell'ingegno grazie alla normativa relativa al diritto d'autore di cui alla legge 633/1941, come modificata successivamente, in particolare sotto tale profilo dal d.lgs. 29 dicembre 1992, n.518, attuazione della direttiva 91/250/CEE del 14 maggio 1991 relativa alla tutela giuridica dei programmi per elaboratore, oggi abrogata e sostituita dalla direttiva 2009/24/CE del 23 aprile 2009, e dal d.lgs. 15 marzo 1996,n.205.

In specifico, sono oggetto di tutela << *i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore*>>, mentre sono esclusi dalla tutela <<*le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce*>>. [31]Sono oggetto di protezione le istruzioni del codice sorgente e del codice oggetto, la struttura, l'organizzazione e la sequenza delle istruzioni e i relativi materiali preparatori.

La legge sulla concorrenza e il mercato, invece, si occupa di regolare l'attività economica per garantire una concorrenza leale e il libero mercato. Nel caso di produttori di App, la legge sulla concorrenza e il mercato può essere rilevante per evitare pratiche commerciali scorrette, come la manipolazione dei prezzi o la pubblicità ingannevole. Inoltre, può essere anche rilevante in caso di fusioni o acquisizioni di aziende che possono avere un impatto sulla concorrenza del mercato.

In generale, i produttori di App devono essere consapevoli di queste leggi e seguire le linee guida appropriate per garantire che la loro applicazione sia conforme alle norme legali e per evitare possibili controversie legali. Inoltre, è importante notare che in caso di violazione delle leggi applicabili, i produttori di App possono essere soggetti a sanzioni amministrative e/o penali. Pertanto, è fondamentale che i produttori di App si informino e seguano le linee guida legali per garantire la conformità e la protezione dei propri interessi, oltre che per tutelare gli utenti finali.

1.1 GDPR e sviluppo di un APP

Nel contesto dello sviluppo di un App, il GDPR impone ai produttori di adottare specifiche misure per garantire la protezione dei dati personali degli utenti.

Il Regolamento prevede che, in base alla finalità del trattamento, il titolare debba fornire agli interessati, prima del trattamento, le informazioni richieste dalle norme[32]. Ciò avviene tramite l'informativa.[33]

La comunicazione delle informazioni sul trattamento dei dati personali risponde al principio di trasparenza e costituisce un obbligo cui, salvo casi eccezionali, sono sottoposti tutti i titolari di trattamento. Essa costituisce un elemento centrale nell'architettura della normativa e il fondamento per l'esercizio dei diritti dell'interessato, che attraverso tali informazioni apprende

[31] Cfr. *Scienza giuridica e tecnologie informatiche,* F. Faini-S. Pietropaoli, Giappichelli, Torino, p.350.

[32] Art.12 GDPR.

[33] L'informativa è una comunicazione rivolta all'interessato che ha lo scopo di rendere edotto il cittadino, anche prima che diventi interessato (cioè prima che inizi il trattamento), sulle finalità e le modalità dei trattamenti operati dal titolare del trattamento.

gli elementi essenziali per l'esercizio dei suoi diritti. Le informazioni devono essere fornite all'interessato al momento della raccolta presso l'interessato o, se i dati sono ottenuti da altra fonte, entro un termine ragionevole, in funzione delle circostanze del caso: se i dati personali potessero essere legittimamente comunicati a un altro destinatario, l'interessato dovrebbe esserne informato nel momento in cui il destinatario riceve la prima comunicazione dei dati personali.[34]

Le informazioni sul trattamento devono essere fornite in maniera concisa, facilmente accessibile e comprensibile e deve essere impiegato un linguaggio semplice e chiaro.[35]

L'informativa deve avere come contenuto minimo quello indicato negli articoli 13 e 14 del Regolamento. All'interno di essa devono essere indicati anche i cookie [36]e nel caso di cookie di terze parti, il link alle pagine delle privacy policy dei servizi delle terze parti.

Inoltre, il titolare del trattamento è tenuto a fornire riscontro, a titolo gratuito, all'istanza dell'interessato senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della stessa richiesta. Specifiche modalità di riscontro alle richieste dell'interessato sono poi contenute nelle disposizioni dedicate ai singoli diritti dell'interessato.[37]

Un altro adempimento posto in capo al titolare e al responsabile del trattamento consiste nella tenuta e nell'aggiornamento periodico del registro delle attività di trattamento. Il registro consiste in un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento. Il titolare, inoltre, è tenuto a fornire la valutazione d'impatto sulla protezione dei dati personali che consiste nella valutazione preventiva dei trattamenti e dei rischi, della necessità dei trattamenti stessi e infine nell'individuazione di misure di sicurezza adeguate.

Nel caso sia avvenuta una violazione dei dati personali, il titolare ha l'obbligo di notificarlo al Garante per la protezione dei dati personali e, ove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche, di comunicarlo anche all'interessato, ai sensi degli artt.33 e 34 del Regolamento. [38]

Le occasioni in cui si richiede la trasmissione di dati agli utenti di App sono molteplici. Durante l'installazione, infatti, l'utente che scarica l'App inserisce informazioni e spesso le stesse App accedono automaticamente a dati memorizzati sul dispositivo per i quali sarebbe necessario chiedere il consenso. Nel caso il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha espresso il consenso. In questo caso, il primo presupposto necessario ad un corretto trattamento è, quindi, ottenere dall'utente il consenso preventivo all'accesso ai dati che va richiesto sia al momento dell'installazione delle App, sia per conservare e gestire i dati personali degli utenti.

La validità del consenso va ottenuta ai sensi della definizione di cui all'articolo 4, n. 11 del GDPR.

Ai sensi dell'art. 7 del GDPR, qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha espresso il consenso al

[34] V.Considerando n.61 del Regolamento.

[35] Cfr.*Diritto di internet,* G.Finocchiaro, Zanichelli ,Bologna ,p.68.

[36] I cookie sono stringhe di testo di piccole dimensioni che i siti visitati dall'utente inviano al suo terminale (solitamente al browser), dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente.

[37] V.artt. da 15 a 22 del Regolamento.

[38] Cfr.*Diritto di internet,* G.Finocchiaro, Zanichelli ,Bologna ,p.73.

trattamento dei propri dati personali.
Inoltre, l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento, senza che ciò pregiudichi la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato viene informato e il consenso può essere revocato con la stessa facilità con cui è stato accordato.
I titolari del trattamento sono tenuti a proteggere i dati personali degli utenti utilizzando misure di sicurezza adeguate, come la crittografia e la protezione da accessi non autorizzati. Questo può includere la creazione di procedure di sicurezza interne, la formazione del personale sulla sicurezza dei dati e la valutazione dei rischi per la sicurezza dei dati.
In caso di violazione della sicurezza dei dati, i titolari sono tenuti a notificare tempestivamente le autorità competenti e gli utenti interessati, in conformità con le disposizioni del GDPR. I titolari devono inoltre avere procedure in atto per gestire e rispondere alle richieste degli utenti di accedere, correggere o eliminare i loro dati personali.[39]

1.2 Protezione dei diritti di proprietà intellettuale

Il software è un bene "immateriale" costituito da un insieme di istruzioni espresse in un qualsiasi linguaggio o codice, atte in modo diretto o indiretto a far eseguire all'elaboratore una funzione e attendere determinati risultati.[40] Le misure giuridiche di tutela, invece, consistono nella protezione offerta dalla disciplina della proprietà intellettuale, che rende escludibile il software subordinando il lecito utilizzo all'autorizzazione del titolare[41].
Il modello giuridico di tutela del software consiste nella protezione quale opera dell'ingegno grazie alla normativa relativa al diritto d'autore di cui alla legge 633/1941. In specifico, sono oggetto di tutela <<i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore>>, mentre sono esclusi dalla tutela <<le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce>>: ciò è coerente con la disciplina del diritto d'autore, che limita la tutela alla forma espressiva dell'opera, quale bene oggetto di protezione giuridica. Il diritto del titolare[42] si compone di diritti morali, irrinunciabili, quale il diritto di paternità(esserne riconosciuto autore), e di diritti patrimoniali, che sono esclusivi del titolare e comportano l'escludibilità , dal momento che le utilizzazioni sono precluse a soggetti diversi se non autorizzati nei limiti e modi che il titolare stabilisce; i diritti esclusivi patrimoniali comprendono la stessa riproduzione del programma permanente o temporanea, totale o parziale, con qualsiasi mezzo o in qualsiasi forma, la traduzione, l'adattamento, la trasformazione e ogni altra modifica

[39] Art. 33 GDPR.

[40] Cfr.G.Finocchiaro*, I contratti aventi ad oggetto il software*, in G.Finocchiaro-F.Delfini (a cura di), op.cit.,p.618 ss.

[41] Cfr.G.Sartor, op.cit.,p.122 ss., che evidenzia un monopolio temporaneo a favore del titolare dei diritti di sfruttamento economico, di lunga durata, dato che si estende fino a sessanta anni dopo la morte dell'autore.

[42] La titolarità spetta all'autore del software e la normativa regola i casi di opere create in rapporto di lavoro dipendente o di opere plurisoggettive, in comune o composte. Cfr.A.M.Gambino-A.Stazi-D.Mula, op.cit.,p.219 ss; D.Sbariscia,op.cit.,p,875 ss..

e qualsiasi forma di distribuzione al pubblico , compresa la locazione.[43] Il titolare dei diritti di utilizzazione economica del programma è l'autore dello stesso. Nel caso in cui l'autore sia un lavoratore dipendente, i diritti di utilizzazione economica del software spettano al datore di lavoro, a meno che non sia stato diversamente pattuito.[44] In Italia vige il divieto di brevettabilità del software ma ci sono delle eccezioni. Il software, infatti, è tutelabile mediante brevetto nel caso in cui non costituisca esso stesso l'oggetto dell'invenzione, ma sia, invece, strumento pet raggiungere il risultato inventivo.[45]

La legge sulla proprietà intellettuale, in relazione allo sviluppo di un App, riguarda il riconoscimento e la protezione dei diritti di proprietà intellettuale legati all' App stessa, come brevetti, marchi, diritti d'autore e segreti commerciali. Per quanto riguarda i diritti d'autore[46], i produttori di App devono essere consapevoli del fatto che il codice sorgente e il design dell'App sono considerati opere dell'ingegno e pertanto protetti dalla legge sul diritto d'autore[47]. Ciò significa che i produttori, in linea di principio, hanno il diritto esclusivo di utilizzare, riprodurre, diffondere e mostrare pubblicamente l'App. In caso di violazione di questi diritti, i produttori possono intraprendere azioni legali per tutelare i loro interessi. Per quanto riguarda i brevetti[48], i produttori di App possono brevettare eventuali innovazioni tecnologiche contenute nell'App, come ad esempio processi, metodi o sistemi innovativi. Ciò può proteggere i produttori dalla riproduzione non autorizzata delle loro idee da parte di altri sviluppatori. Per quanto riguarda i marchi[49], i produttori di App possono registrare il nome dell'App come marchio per tutelare la loro reputazione e distinguere la loro App da quelle di altri produttori. Inoltre, i produttori di App devono essere consapevoli che l'utilizzo di contenuti protetti da diritto d'autore, come immagini o musica, senza le adeguate autorizzazioni può comportare sanzioni legali. Inoltre, è importante notare che, in alcuni casi, l'utilizzo di un'idea o di una tecnologia già esistente può costituire una violazione delle leggi sulla proprietà intellettuale. I produttori di App dovrebbero pertanto sempre condurre un'adeguata ricerca sulla disponibilità di brevetti, marchi e diritti d'autore prima di utilizzare un'idea o una tecnologia nella loro App. In generale, è importante che gli sviluppatori di App siano consapevoli delle leggi sulla proprietà intellettuale e seguano le linee guida appropriate per proteggere i propri diritti ed evitare possibili controversie legali.

[43] Cfr. *Scienza giuridica e tecnologie informatiche,* F.Faini-S.Pietropaoli,Giappichelli,Torino,p.348.

[44] Cfr. *Diritto di internet,* G.Finocchiaro, Zanichelli ,Bologna ,p.196.

[45] Cfr. *Diritto di internet,* G.Finocchiaro, Zanichelli ,Bologna ,p.198.

[46] Il diritto d'autore tutela le opere dell'ingegno di carattere creativo riguardanti le scienze, la letteratura, la musica, le arti figurative, l'architettura, il teatro, la cinematografia, la radiodiffusione e, da ultimo, i programmi per elaboratore e le banche dati, qualunque ne sia il modo o la forma di espressione.

[47] L.633/1941.

[48] Attestato, concesso da apposito ufficio, che garantisce la priorità e il diritto esclusivo di sfruttamento industriale di un'invenzione, oppure l'uso di un marchio d'impresa o di un modello.

[49] Segno indelebile di riconoscimento.

1.3 La legge sulla concorrenza e il mercato

È stato osservato che le nuove tecnologie digitali hanno aggravato notevolmente il problema del coordinamento tra imprese.[50]L'evoluzione tecnologica ha fortemente facilitato sia lo scambio di informazioni tra imprese, concorrenti e no, sia il monitoraggio reciproco dei comportamenti di mercato tenuti da ciascuna delle parti di un accordo anticoncorrenziale.[51]
La legge sulla concorrenza e il mercato mira a garantire una concorrenza leale tra le imprese e un libero mercato per i consumatori.

Nel contesto dello sviluppo di un App, questa legge può essere rilevante per evitare pratiche commerciali scorrette, come la manipolazione dei prezzi o la pubblicità ingannevole. Inoltre, può essere anche rilevante in caso di fusioni o acquisizioni di aziende che possono avere un impatto sulla concorrenza nel mercato delle App. I produttori di App devono essere consapevoli delle leggi e delle regole sulla concorrenza e il mercato e aderire a esse per evitare sanzioni legali. Ciò può includere la valutazione della concorrenza nel mercato delle App prima di lanciare un App, o l'acquisizione di un'altra azienda che sviluppa App, e adottare misure per garantire che l'acquisizione non violi le leggi sulla concorrenza e il mercato. Inoltre, i produttori devono essere consapevoli delle leggi e delle regole sulla pubblicità e la promozione delle loro App per evitare di ingannare i consumatori o di violare le leggi sulla concorrenza e il mercato. Per quanto riguarda la distribuzione delle App, i produttori devono essere consapevoli delle leggi e delle regole sulla concorrenza e il mercato in merito alle condizioni imposte dagli store di App e adottare misure per garantire che le condizioni non violino le leggi sulla concorrenza e il mercato. In generale, i produttori devono sempre aderire alle leggi sulla concorrenza e il mercato per evitare sanzioni legali e garantire una concorrenza leale nel mercato delle App. È importante che i produttori lavorino con avvocati specializzati in questo campo per garantire che le loro attività soddisfino tutti i requisiti legali e per evitare possibili controversie.

2. Linee guida per la conformità alla normativa

Per garantire la conformità alla normativa nel processo di sviluppo di un App, i produttori delle stesse dovrebbero seguire alcune linee guida. Innanzitutto, dovrebbero informarsi e comprendere le leggi applicabili citate in precedenza; dopodiché è necessario creare una privacy policy [52]per informare gli utenti su come vengono utilizzati i propri dati personali e per ottenere il loro consenso.

L'informativa privacy dovrà indicare l'identità del titolare del trattamento (proprietario dell'App), le precise categorie di dati personali oggetto di raccolta e trattamento; per quali finalità vengono trattati i dati personali; se i dati saranno divulgati a terzi; in che modo l'utente può esercitare i suoi diritti previsti dal GDPR, in particolare su revoca e cancellazione dei dati.
L'informativa sul trattamento dei dati personali ai sensi degli artt. 13 e 14 GDPR deve essere

[50] Cfr. Quarta A.- Smorto G. ,*Diritto privato dei mercati digitali*, Firenze, 2020, p.161 ss.
[51] Cfr.*Diritto dell'innovazione,* A.Blandini, CEDAM ,Milano ,p.216.

[52] La Privacy Policy è un documento, redatto all'interno del sito, che informa gli utenti circa il trattamento dei loro dati personali.

fornita in modo trasparente. Il titolare del trattamento è tenuto a trasmettere le informazioni rilevanti con chiarezza e concisione, evitando formulazioni articolate e complesse che non pongano l'interessato in condizioni di comprendere da parte di chi, in che modo e per quali finalità siano trattati i propri dati personali. Il titolare deve tenere conto anche degli specifici soggetti cui le informazioni sono rivolte, adottando un registro linguistico consono e ponendo una particolare cura in caso di informazioni destinate a minori o ad altri soggetti vulnerabili. Quanto all'accessibilità, le informazioni devono essere rese disponibili agli interessati facilmente e separatamente da altre informazioni, laddove queste siano fornite insieme.[53] La disponibilità di queste informazioni è fondamentale per ottenere un consenso valido da parte dell'utente, ove necessario. La comunicazione di tali informazioni solo dopo che l'applicazione ha avviato il trattamento dei dati personali (spesso già durante l'installazione) non è ritenuta sufficiente, né legalmente valida ai sensi del GDPR. Infine, la privacy policy dell'App dovrebbe differenziare chiaramente le informazioni obbligatorie e quelle facoltative e il sistema dovrebbe consentire all'utente di rifiutare l'accesso alle informazioni facoltative utilizzando opzioni predefinite rispettose della privacy.

Oltre a quanto già detto, i produttori, devono utilizzare misure di sicurezza adeguate a proteggere i dati personali degli utenti, come la crittografia e la protezione da accessi non autorizzati. Sono misure di sicurezza organizzative le attività e gli adempimenti svolti per assicurare l'applicazione del GDPR e la riduzione dei rischi derivanti dal trattamento dei dati (es. l'adesione a un codice di condotta o l'uso di un meccanismo di certificazione degli accessi).

Le misure di sicurezza previste dal GDPR devono essere adottate dal titolare e dal responsabile del trattamento in modo adeguato al caso concreto. Non esiste un elenco di misure da adottare, tuttavia, il Regolamento europeo GDPR prevede alcune misure di sicurezza a titolo esemplificativo come la cifratura e pseudonimizzazione: ad esempio, l'uso di algoritmi per la cifratura dei dati salvati e l'anonimizzazione dei dati per garantire la confidenzialità; garanzia di riservatezza: ad esempio, con la restrizione degli accessi, monitoraggio degli accessi, firewall, password e credenziali sicure ; garanzia di integrità, disponibilità, resilienza e ripristino tempestivo: ad esempio, l'adozione di meccanismi di backup o particolari tipologie di archiviazione dei dati (archiviazione ridondante); procedure di verifica per testare l'efficacia delle misure adottate: ad esempio, audit indipendenti per la verifica e il controllo sulla compliance privacy. [54][55]

Le regole sulle misure di sicurezza introdotte dal GDPR sono utili anche per minimizzare i danni e i rischi derivanti da una violazione dei dati personali. Infatti, se si verifica una violazione di sicurezza, i dati possono essere distrutti, divulgati o rubati in modo non autorizzato. In questi casi, il titolare del trattamento deve documentare tutte le violazioni e nei casi più gravi notificare la violazione al Garante per la protezione dei dati personali (es. in caso di furto di identità o di un danno alla reputazione dell'interessato). Il Garante della privacy se rileva una violazione del GDPR che riguarda le misure di sicurezza può prescrivere misure correttive e sanzioni economiche. Tali sanzioni possono arrivare fino a fino a €10 milioni oppure fino al 2% del fatturato totale annuo mondiale. Per questo è molto importante adottare tutte le misure di sicurezza adeguate al trattamento dei dati personali.

Notificare le autorità competenti: in caso di violazione della sicurezza dei dati, i produttori devono

[53] Cfr. *Privacy e data Protection 2022*, Giulio Coraggio, IPSOA, Milano, p.20.

[54] Art.32 del GDPR.

[55] Cfr. Privacy e data Protection 2022, Giulio Coraggio, IPSOA, Milano, p.217.

notificare le autorità competenti e gli utenti interessati. Gli sviluppatori devono consentire agli utenti di accedere, correggere o eliminare i loro dati personali in conformità alle leggi sulla protezione dei dati personali; devono tenere traccia dei consensi degli utenti per garantire la conformità alle leggi sulla protezione dei dati personali.

L'informativa privacy dell'App deve informare per quanto tempo verranno conservati i dati personali. L'informativa privacy dovrebbe quindi indicare un periodo di tempo di inattività dopo il quale l'account sarà considerato scaduto e garantire che l'utente ne sia informato. Alla scadenza di tale periodo di tempo, il titolare del trattamento dovrebbe avvertire l'utente e dargli la possibilità di recuperare i dati personali. Se l'utente non rispondesse, i suoi dati personali e relativi all'utilizzo dell'applicazione dovrebbero essere resi anonimi o cancellati in modo irreversibile.

I produttori di App dovrebbero anche essere consapevoli dei requisiti di conformità per quanto riguarda la pubblicità e la promozione dell'App, inclusi i requisiti per le recensioni degli utenti e la pubblicità mirata. Inoltre, i produttori devono essere consapevoli delle leggi e delle regole sulla tutela dei minori e sulla protezione dei dati dei minori, come ad esempio la richiesta di un consenso da parte dei genitori per il trattamento dei dati personali dei minori. Infine, i produttori dovrebbero tenere traccia delle modifiche alle leggi e alle regole applicabili e adeguare di conseguenza la loro App e le loro pratiche di conformità in modo tempestivo. In generale, è importante per i produttori seguire costantemente le linee guida per la conformità alla normativa per garantire che l'App sia conforme alle leggi e alle regole e per proteggere i diritti degli utenti e gli interessi dei produttori stessi.

3.Come le tecnologie emergenti stanno influenzando le questioni legali relative allo sviluppo di app

Le tecnologie emergenti come l'intelligenza artificiale, il cloud computing, l'Internet delle cose e la blockchain stanno rapidamente cambiando il modo in cui le aziende raccolgono, utilizzano e conservano i dati. Queste tecnologie stanno anche creando nuove sfide per quanto riguarda la conformità alle leggi sulla protezione dei dati personali e sulla privacy.

Per quanto riguarda l'intelligenza artificiale, ad esempio, ci sono preoccupazioni per la trasparenza e la responsabilità delle decisioni prese dai sistemi automatici, nonché per l'utilizzo etico dei dati personali per addestrare i modelli. Inoltre, l'intelligenza artificiale può anche creare nuove questioni legali riguardo al bias nei dati [56]e al diritto alla spiegabilità delle decisioni. In determinate circostanza anche l'acquisizione di un'enorme mole di dati, basati o meno sul linguaggio naturale ed elaborati da un calcolatore, non è sufficiente ad evitare che l'IA produca discriminazioni e ingiustizie nella soluzione di problemi umani. Si tratta cioè degli effetti di Biased model o di algoritmi di Machine Learning distorti, che possono portare ad un trattamento ingiusto e comportare danni e discriminazioni, non solo nei confronti di un individuo ma addirittura per un particolare gruppo sociale, in specie se minoritario e vulnerabile. L'IA è bensi' in grado di sviluppare ragionamenti utili a risolvere problemi complessi, ma può accadere che essa non sia in grado di rispondere efficacemente a talune necessità umane, anche se i dati raccolti

[56] si riferisce alla situazione in cui i sistemi di analisi dei dati basati sui sistemi di Machine Learning mostrano atteggiamenti discriminatori nei confronti di determinati gruppi di persone.

vengono completati con sistemi di Natural Language Processing (NLA), cioè con tecnologie che consentono all'uomo di interagire con le macchine, sfruttando il linguaggio naturale.[57]

Il cloud computing, d'altra parte, solleva criticità relative alla data governance, in particolare sotto i profili dell'integrità, della sicurezza e del controllo dei dati, per i quali risultano necessarie la definizione di standard e la previsione dei livelli di servizio, attraverso impegni specifici, puntuali verifiche e definite responsabilità. A livello giuridico, infatti, gli insiemi di dati e informazioni conferiti in cloud sollevano una serie di possibili problematiche diverse in base alle fattispecie concrete, potendo involgere aspetti di proprietà intellettuale e di segreto industriale e correlate potenziali violazioni degli stessi.[58]

L'Internet delle cose, infine, solleva preoccupazioni per la sicurezza dei dati personali raccolti da dispositivi connessi e la loro utilizzo non autorizzato, compreso l'accesso non autorizzato ai dati e la possibilità di utilizzare i dati per scopi illeciti.

Per rispondere a queste sfide, i produttori dovrebbero essere a conoscenza delle leggi e delle linee guida sulla protezione dei dati personali e sulla privacy, tra cui il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea e il California Consumer Privacy Act (CCPA) negli Stati Uniti. Inoltre, i produttori dovrebbero adottare misure di sicurezza adeguate a proteggere i dati personali degli utenti, come la crittografia e la protezione da accessi non autorizzati, e considerare l'adozione di tecnologie come la crittografia e la protezione da accessi non autorizzati. Inoltre, è importante per i produttori di App essere consapevoli dei rischi specifici associati alle diverse tecnologie emergenti e adottare misure per mitigare questi rischi. Ad esempio, per l'utilizzo dell'intelligenza artificiale, i produttori dovrebbero considerare l'implementazione di meccanismi di spiegazione per rendere trasparenti le decisioni prese dai modelli e garantire che non siano basate su pregiudizi o bias. Per quanto riguarda il cloud computing, i produttori dovrebbero valutare i provider di servizi cloud per verificare che siano conformi alle norme e alle leggi sulla protezione dei dati. I produttori dovrebbero essere pronti ad adattarsi a eventuali cambiamenti futuri nella normativa, tenendo in considerazione le nuove tecnologie emergenti e come queste possono influire sulla protezione dei dati personali e sulla privacy degli utenti.

[57] Cfr. *Diritto costituzionale e nuove tecnologie*, G.Ferri, Edizioni Scientifiche Italiane, Verona, p.268.
[58] Cfr. *Scienza giuridica e tecnologie informatiche,* F. Faini-S. Pietropaoli, Giappichelli, Torino, p.402.

CAPITOLO 3

EMERGENZA SANITARIA: APP IMMUNI E IL RISPETTO DELLA PRIVACY

Sommario: 1. Come funziona l'app - 2. Quali dati vengono trattati –3. Bilanciamento fra diritto alla salute pubblica e diritto alla riservatezza – 4. Conservazione dei dati

1. Come funziona l'app

Immuni è un App dedicata al trattamento dei dati personali con il solo fine di allertare le persone che siano entrate in contatto stretto (di prossimità) con soggetti risultati positivi al fine di tutelare la loro salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenzaCovid-19.

La Piattaforma unica nazionale gestisce il sistema sopra menzionato e consente di inviare le notifiche, attraverso un sistema di alert, a coloro i quali abbiano scaricato e installato, su base volontaria, la predetta App.

L'App Immuni si fonda sulla tecnologia Bluetooth Low Energy (BLE) e mantiene i dati dell'utente sul proprio dispositivo, assegnandogli un ID temporaneo, che varia spesso e viene scambiato tramite Bluetooth con i dispositivi vicini. Il tracciamento avviene in quattro step successivi. In primo luogo, i telefoni cellulari conservano in memoria i dati di altri cellulari con cui sono entrati in contatto via Bluetooth, in forma di codicianonimi crittografati. Associati a questi codici ci sono i metadati (durata dell'incontro tra dispositivi, forza del segnale percepito) che entrano in gioco nella valutazione, che viene effettuata direttamente in locale sul singolo device, del "rischio contagio". In secondo luogo, quando uno dei soggetti che ha scaricato l'applicazione risulta positivo al virus, gli operatori sanitari gli forniscono un codice di autorizzazione con il quale questi può scaricare su un server ministeriale il proprio codice anonimo.

In terzo luogo, i cellulari con l'app prendono a intervalli regolari dal server i codici dei contagiati. In quarto luogo, se l'app riconosce tra i codici nella propria memoria un codice di contagiato, visualizza la notifica all'utente.

La trasmissione dei dati è cifrata e firmata digitalmente per garantire la massima sicurezza e riservatezza in questa fase di "uscita" del dato dallo smartphone del singolo utente.

A ogni contatto viene associato un indice di rischio calcolato in base a parametri come la distanza (che è sempre approssimata e dipende statisticamente dalla potenza del segnale rilevato) e dal tempo di contatto.[59]

Ogni Paese stabilisce i parametri da cui desumere se il contatto è stato a rischio oppure no. Il

[59] L'indice di rischio del contagio è elaborato attraverso l'algoritmo messo a disposizione da Apple e da Google, che esamina due parametri: l'intensità del segnale Bluetooth (che attesterebbe la vicinanza del contatto), e la durata del contatto. Approssimativamente, pertanto, possiamo dire che più lungo è il contatto e più intenso è il segnale Bluetooth e maggiore sarà l'indice di rischio.

Ministero dellaSalute ha individuato i parametri del rischio, per fare scattare l'avviso nei seguenti: oltre 15 minuti di contatto; a meno di due metri. Se l'indice di rischio supera una soglia predefinita e il contatto è avvenuto conun soggetto poi risultato positivo al virus, l'applicazione mostrerà all'utente un messaggio di allerta "sulla possibile esposizione al contagio", la cosiddetta "notifica di esposizione" e fornisce consigli su cosa fare dopo(ad esempio, isolarsi e chiamare il proprio medico di famiglia).

Oltre a queste informazioni relative al sospetto di contagio, l'App raccoglie quotidianamente ulteriori informazioni, definite analytics di tipo Operational info[60], che trasmette automaticamente al sistema, finalizzate a comprendere la diffusione dell'utilizzo dell'App sul territorio nazionale e il suo corretto utilizzo.

A tal fine sono raccolti dati relativi: alla provincia di domicilio, al sistema operativo utilizzato (IOS o Android), all'attivazione o meno del Bluetooth, alla concessione delle autorizzazioni di notifica del rischio di contagio, all'avvenuta ricezione o meno, e quando, di notifiche di sospetto contagio. Attualmente la trasmissione di tali informazioni riguarda solo i dispositivi con sistema operativo IOS(Apple), in quanto unico sistema che consente di verificare l'autenticità del dispositivo dal quale provengono i dati[61].

Il testo dell'informativa agli interessati, resa dal Titolare (Ministero della salute) ai sensi degli artt.13 e 14 del Regolamento, in relazione al trattamento dei dati personali, risponde ai principi sanciti ai sensi di cui all'Art.5e 6 GDPR.

Il Titolare, inoltre, che opera attraverso un sistema di backend e attraverso un servizio di interazione con gli operatori sanitari mediante utilizzo del Sistema Tessera Sanitaria, si avvale, altresi', di Sogei S.p.A. e del MEF,limitatamente a tale sistema, agendo questi ultimi in qualità di soggetti responsabili (Art.28 GDPR).

L'App, relativamente ai sistemi tecnologici utilizzati e con riferimento alle misure tecniche e organizzative adottate, appare idonea a garantire un adeguato livello di sicurezza e, in particolare: la descrizione del sistema di allerta Covid-19.[62]

L'app Immuni funziona senza la necessità di creare un account e richiede l'autorizzazione dell'utente per l'attivazione delle funzionalità necessarie, come il Bluetooth. L'app utilizza algoritmi crittografici per generareuna chiave temporanea giornaliera, denominata TEK, da cui vengono generati identificativi di prossimità deldispositivo mobile, noti come RPI, che vengono diffusi tramite Bluetooth. Gli RPI dei dispositivi con cui l'utente è entrato in contatto vengono memorizzati localmente insieme ad altri dati accessori e vengono cancellati dopo 14 giorni. In caso di positività al COVID-19, l'utente può fornire le proprie TEK a un operatoresanitario che le

[60] L'espressione "analytics di tipo Operational info" si riferisce a informazioni raccolte e analizzate al fine di comprendere l'efficacia e l'uso corretto di un sistema o di un'applicazione. In particolare, si tratta di dati relativi all'operatività dell'applicazione, come l'uso delle sue funzionalità, la tipologia di dispositivo e sistema operativo utilizzato, l'attivazione di determinate autorizzazioni o notifiche, e altre informazioni utili a migliorare il funzionamento dell'app e a monitorarne la diffusione sul territorio. Questi dati sono utilizzati per valutare l'efficaciadell'applicazione e per individuare eventuali problematiche da risolvere.

[61] Cfr. C.Baldassarre,*L 'App Immuni al banco di prova, tra rispetto della privacy e difesa della salute pubblica*, Roma, 2020.

[62] Cfr. M.Festa, *Ultimo capitolo della saga IMMUNI: l'App, autorizzata dal Garante, è finalmente negli store*, Milano, 2020.

caricherà nel sistema Immuni per avvertire gli utenti che sono stati a contatto con il pazienteinfetto. Il meccanismo di autorizzazione e caricamento delle TEK è progettato per garantire la sicurezza e la privacy dei dati degli utenti.

2.Quali dati vengono trattati

L'applicazione viene installata liberamente e volontariamente dagli interessati, e consente a questi ultimi di essere informati attraverso un alert solo laddove siano entrati in contatto di prossimità con un soggetto risultato positivo al Covid-19, consigliando altresi' di rivolgersi al proprio medico.

Il Sistema di allerta Covid-19, oltre alle TEK (Temporary Exposure Key) degli utenti accertati positivi al Covid-19, raccoglie, attraverso l'app, le ulteriori informazioni di seguito descritte.

Ogni qual volta un utente risultato positivo al Covid-19 decide, liberamente, al fine di "avvisare altri utenti arischio di contagio", di effettuare il caricamento delle proprie TEK su sistema di backend, comunicando all'operatore sanitario la data di inizio dei sintomi, l'App trasmette automaticamente anche ulteriori informazioni chiamate Epidemiological Info al backend di Immuni. In tale circostanza vengono raccolti sul sistema si allerta Covid-19, come impostazione predefinita, i dati sotto specificati per "consentire l'affinamento dell'algoritmo di calcolo del rischio derivante da un contatto e allertare solo le persone che sono effettivamente a rischio", nonché per "finalità di tutela della salute pubblica" e "di carattere epidemiologico". Le informazioni epidemiologiche includono la provincia di domicilio e il riassunto della rilevazione dell'esposizione[63] ovvero : il numero di contatti a rischio rilevati, il numero di giorni trascorsi dall'ultimo contatto a rischio, la durata aggregata dei contatti a rischio (misurata in multipli di 5 min. fino a un massimo di 30 min.), la distinzione per tre intervalli di intensità del segnale bluetooth (chiamata attenuation) e l' indice di rischio più elevato tra quelli relativi ai contatti a rischio.

Inoltre,ci sono le Exposure Info, ossia una serie di informazioni analitiche relative a ciascun eventuale contatto a rischio avvenuto negli ultimi 14 giorni (rilevato attraverso il raffronto delle TEK scaricate con gli RPI memorizzati all'interno del dispositivo), che comprendono: la data in cui è avvenuto il contatto a rischio,durata del contatto a rischio (misurata in multipli di 5 min fino a un massimo di 30 min), l'intensità del segnaleBluetooth durante il contatto a rischio (chiamata attenuation),la durata del contatto a rischio (misurata in multipli di 5 min fino a un massimo di 30 min), la distinzone per tre intervalli di intensità del segnale Bluetooth(chiamata attenuation), il rischio di contagiosità associato alla TEK relativa al contatto a rischio e l'indice di rischio relativo al contatto a rischio.

L'App trasmette in modo automatico al backend di Immuni le Operational Info without Exposure e, se c'è stato un contatto a rischio, le Operational Info with Exposure.

Il numero di invii di analytics di tipo OperationalInfo che un singolo dispositivo può effettuare è limitato su base mensile. Le Operational Info vengono raccolte per "capire statisticamente il livello di diffusione dell'app sul territorio e la correttezza del suo utilizzo", nonché per

[63] una serie di informazioni sintetiche relative a tutti gli eventuali contatti a rischio avvenuti negli ultimi 14 giorni.

"monitorare su base statistica l'epidemia, allocare in modo più efficiente le risorse sanitarie e massimizzare quindi la prontezza e l'adeguatezza del supporto fornito agli utenti che risultano a rischio". Allo stato attuale, la trasmissione di tali analytics riguarda unicamente i dispositivi con sistema operativo iOS. Infatti, al fine di garantire la validità delle Operational Info e di imporre un limite mensile al loro invio da parte dei dispositivi mobili, evitando nel contempo l'eventuale inquinamento dei dati raccolti dal backend, il Sistema di allerta Covid-19 fa ricorso a tecniche di device attestation che consentono di verificare l'autenticità del dispositivo dal quale provengono i dati. Tuttavia, queste tecniche sono attualmentepossibili solo per dispositivi con sistema operativo iOS (API DeviceCheck di Apple).

Le Operational Info comprendono: analytics token , provincia di domicilio, stato di attivazione dell'interfaccia bluetooth, stato del permesso all'utilizzo del Framework A/G per la notifica di esposizione, stato del permesso alla visualizzazione di notifiche locali generate dall'app, sistema operativo del dispositivo mobile (iOS o Android), avvenuta ricezione o meno di notifiche di esposizione al rischio, data in cui è eventualmente avvenuta l'ultima esposizione al rischio (contatto stretto con un soggetto risultato positivo).

Al fine di consentire al backend di Immuni di verificare l'autenticità dei dispositivi dai quali provengono gli analytics di tipo Operational Info, per i soli dispositivi con sistema operativo iOS, vengono effettuate le seguenti operazioni: l'app Immuni richiede ad Apple ("DeviceCheck iOS API") l'attribuzione di un identificativo temporaneo del dispositivo, denominato device token, che consentirà al backend di Immuni diverificarne l'autenticità. Successivamente, l'app Immuni genera, in modo casuale, un altro identificativo del dispositivo, denominato analytics token, salvandolo in locale e inviandolo al backend di Immuni unitamenteal device token attribuito da Apple. Alla ricezione di tali dati, il backend di Immuni verifica con Apple ("DeviceCheck server API") la validità del device token relativo al dispositivo dell'utente. In tale circostanza, il backend di Immuni si avvale anche di alcune funzionalità rese disponibili da Apple (c.d. "DeviceCheck per- device bits") che consentono di tenere traccia di quei dispositivi mobili che, avendo assunto un comportamento anomalo nella generazione dell'analytics token, non sono autorizzati a inviare Operational Info. In caso di riscontro positivo da parte del servizio di Apple, il backend di Immuni memorizza l'analytics token in un database, associandolo a un contatore di invii. Ogni qual volta l'app Immuni deve inviare gli analytics di tipo Operational Info, viene trasmesso l'analytics token generato in precedenza. Il backend di Immuni, al ricevimento dei dati Analytics, controlla se l'Analytics token esiste, se è stato generato e se non ègià stato utilizzato per effettuare due invii. Solo se tutte queste condizioni sono soddisfatte, le Operational Info vengono accettate e salvate nel database di Immuni. In caso contrario, i dati vengono scartati. L'analyticsToken cambia con cadenza mensile e viene inviato al backend di Immuni al massimo tre volte al mese, in modo da limitare "la capacità del server di reidentificare lo stesso dispositivo a cavallo di più chiamate al server". Su base mensile i dispositivi su cui è istallata l'app Immuni generano, in modo casuale, un identificativo denominato Analytics token necessario a verificare la validità degli Analytics di tipo Operational Info inviati al Sistema di allerta Covid-19[64].

[64] Cfr. *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid19-App Immuni* ,1° giugno 2020, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9356568.

3.Bilanciamento fra diritto alla salute pubblica e diritto alla riservatezza

L'improvviso scoppio della pandemia COVID-19 ha costretto i governi di tutto il mondo a prendere misure drastiche per proteggere la salute pubblica, spesso a discapito delle libertà individuali. In particolare, si è reso necessario trovare un equilibrio tra il diritto alla salute pubblica e il diritto alla riservatezza, in quanto la lottacontro la diffusione del virus richiede il monitoraggio dei cittadini attraverso la raccolta e l'elaborazione di dati personali sensibili.

In Italia, una delle iniziative introdotte per contrastare la diffusione del virus è stata lo sviluppo di un'applicazione di contact tracing. Tuttavia, l'utilizzo di tale App ha sollevato alcune questioni riguardanti il bilanciamento tra il diritto alla salute pubblica e il diritto alla riservatezza.

Il diritto alla riservatezza è strettamente legato alle trasformazioni della società post-industriale, come il maggiore contatto tra individui estranei l'uno all'altro, la circolazione delle persone in ambienti indipendentie l'uso crescente di tecnologie di raccolta dati. Questi elementi possono compromettere la privacy delle persone e richiedere difese adeguate. L'uso delle reti informative e delle banche dati crea problemi di grande rilievo, perché il trattamento delle informazioni riguardanti la salute può essere utile per risolvere patologiee contribuire al progresso scientifico, ma anche lesivo del diritto alla riservatezza.

Il diritto alla salute può essere visto come un diritto-dovere del singolo soggetto di mettere a disposizione leinformazioni sulla propria salute per garantire prestazioni sanitarie più efficienti e per contribuire al progresso scientifico. Tuttavia, il progresso scientifico richiede la raccolta, conservazione ed elaborazione deidati sanitari, che possono essere sensibili e richiedere adeguati livelli di tutela della privacy.

Durante l'emergenza pandemica, il bilanciamento tra il diritto alla salute pubblica e il diritto alla riservatezzaè stato ancora più difficile perché i dati sensibili costituivano una fonte fondamentale per la costruzione di un sistema di prevenzione e contenimento della diffusione del virus, ma anche una fonte di conoscenza scientifica e di progresso nel campo sanitario. La questione della prevalenza del diritto alla salute rispetto alla riservatezza è stata risolta in favore del primo, perché la tutela della sicurezza pubblica è stata considerata prioritaria rispetto all'interesse individuale alla riservatezza.[65]

La Corte costituzionale italiana ha chiarito che nessun diritto fondamentale è incomprimibile, compreso quello alla riservatezza, ma tale diritto può essere limitato qualora il provvedimento legislativo che realizza tale compressione risponda ai principi di proporzionalità, necessità ed idoneità. In altre parole, le limitazionialla riservatezza possono essere giustificate solo se sono proporzionali allo scopo per cui vengono adottate, necessarie per raggiungere tale scopo e idonee a conseguire il risultato prefissato. In questo contesto, l'applicazione di contact tracing sviluppata in Italia si è mostrata rispettosa del principio di minimizzazione e della privacy degli utenti, ma poco efficiente nell'individuazione dei contatti a rischio di contagio. Tuttavia, la possibilità di rendere obbligatorio l'utilizzo dell'app di tracing avrebbe potuto scongiurare, almeno in parte, i danni arrecati all'economia italiana.

D'altronde, è importante sottolineare che la sorveglianza attiva della popolazione attraverso l'utilizzo di tecnologie di tracciamento deve essere bilanciata con il rispetto dei diritti fondamentali dei cittadini, tra cui il diritto alla riservatezza. In particolare, è necessario che le

[65] Cfr. C.Baldassarre,*L 'App Immuni al banco di prova, tra rispetto della privacy e difesa della salute pubblica*, Roma,2020.

autorità preposte alla raccolta e all'elaborazione dei dati personali agiscano nel rispetto della normativa in materia di tutela della riservatezza e delle indicazioni fornite dalle autorità di regolamentazione a livello europeo, come l'EDPB[66].

Infine, è importante considerare che la crisi economica causata dalla pandemia ha colpito in modo particolarele piccole e medie imprese, che costituiscono la spina dorsale dell'economia italiana. Pertanto, le misure adottate per contrastare la diffusione del virus non possono basarsi esclusivamente sulla chiusura degli esercizi commerciali, ma devono tener conto delle conseguenze economiche e sociali delle limitazioni alla circolazione e alle attività produttive.[67]

In ogni caso, la pandemia ha evidenziato la necessità di trovare un equilibrio tra il diritto alla salute pubblicae quello alla riservatezza. È importante sottolineare che tali diritti non sono in contrasto l'uno con l'altro, ma possono e devono essere armonizzati per garantire il benessere collettivo senza sacrificare le libertà individuali. In tal senso, le innovazioni tecnologiche possono rappresentare un'importante risorsa per la prevenzione e la gestione delle epidemie, ma il loro impiego deve avvenire nel rispetto delle norme in materiadi protezione dei dati personali e della dignità umana. La pandemia, quindi, rappresenta una grande sfida peril nostro sistema giuridico e per la società nel suo complesso, ma può anche essere un'occasione per rafforzare i principi fondamentali della democrazia e per promuovere una cultura della solidarietà e della responsabilità sociale.

4. Conservazione dei dati

La questione della conservazione dei dati nell'app Immuni è stata al centro del dibattito sulla privacy e la tutela dei dati personali durante la pandemia da COVID-19. L'applicazione, sviluppata dal governo italiano per tracciare i contatti dei soggetti positivi al virus, raccoglie una serie di informazioni personali degli utenti,come il codice fiscale, il numero di telefono e la data di nascita, oltre a informazioni sulle interazioni con altri utenti dell'App.

L'aspetto più controverso della conservazione dei dati riguarda il fatto che, inizialmente, la conservazione avveniva sui server di Amazon Web Services (AWS), una società di proprietà di Amazon.com Inc. L'utilizzo di server di una società privata per la conservazione dei dati personali degli utenti dell'app Immuni ha sollevato dubbi sulla sicurezza e la riservatezza dei dati.

Successivamente, il governo italiano ha deciso di spostare i server di conservazione dei dati su infrastrutture nazionali, gestite dal Consiglio Nazionale delle Ricerche (CNR) e da altre società italiane. Tuttavia, anche questa soluzione non è stata priva di critiche, poiché è stata sollevata la questione della sicurezza e dell'affidabilità di tali infrastrutture.
È importante sottolineare che la conservazione dei dati nell'App Immuni avviene in conformità alle normative europee sulla protezione dei dati personali, in particolare al Regolamento Generale sulla Protezione dei Dati (GDPR), che prevede il principio di minimizzazione dei dati e la

[66] L'EDPB (European Data Protection Board) è un organismo indipendente dell'Unione Europea composto dalle autoritànazionali per la protezione dei dati e dal Garante europeo della protezione dei dati. L'EDPB è stato creato dal Regolamento generale sulla protezione dei dati (GDPR) al fine di garantire la coerenza dell'interpretazione e dell'applicazione del GDPR in tutti gli Stati membri dell'UE. L'EDPB fornisce anche consulenza sulla protezione dei dati alle istituzioni dell'UE e ai singoli Stati membri, nonché alle parti interessate.

[67] Cfr. A.Cinque, *Privacy, Big-data e contact tracing: il delicato equilibrio fra diritto alla riservatezza ed esigenze di tuteladella salute,*Roma,2020.

necessità di una conservazione limitata nel tempo dei dati personali. Secondo questi principi, i dati personali devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati", e "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalitàper le quali sono trattati".[68]

L'art. 6, comma 6, del d.l. n. 28/2020 prevede che l'utilizzo dell'App e della piattaforma, nonché ogni trattamento di dati personali effettuato tramite di essi devono essere interrotti alla data di cessazione dellostato di emergenza disposto con delibera del Consiglio dei ministri del 31 gennaio 2020, e comunque non oltre il 31 dicembre 2020. Entro tale data tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi. Inoltre, i dati relativi ai contatti stretti sono conservati, anche nei dispositivi mobilidegli utenti, per il periodo strettamente necessario al trattamento, la cui durata è stabilita dal Ministero dellasalute e specificata nell'ambito delle misure di cui al presente comma; i dati sono cancellati in modo automatico alla scadenza del termine [69].

Il Ministero della Salute ha indicato specifici tempi di conservazione dei dati personali in relazione alle finalitàspecifiche, prevedendo la cancellazione dei dati personali una volta esaurita la finalità per i quali sono stati raccolti e comunque non oltre il 31 dicembre 2020. Inoltre, per valutare la proporzionalità del trattamento effettuato, è importante sottolineare che le TEK e gli RPI memorizzati sui dispositivi mobili degli utenti sono cancellati automaticamente dopo 14 giorni, mentre le TEK dei soggetti risultati positivi Covid-19 che hanno effettuato l'upload sul backend di Immuni sono analogamente cancellate dopo 14 giorni.

Inoltre, l'App Immuni utilizza la tecnologia di tracciamento basata sul protocollo decentralizzato di Google eApple, che garantisce un'ulteriore tutela della privacy degli utenti.

Nonostante questi sforzi per garantire la sicurezza e la privacy dei dati degli utenti dell'app Immuni, è importante che vengano adottate misure adeguate a prevenire eventuali violazioni della sicurezza dei dati eper garantire il rispetto della privacy degli utenti. A tal fine, il garante per la protezione dei dati personali ha emanato una serie di linee guida per l'utilizzo delle applicazioni di contact tracing durante la pandemia.

In sintesi, la conservazione dei dati nell'app Immuni è stata oggetto di un dibattito acceso durante la pandemia da COVID-19, ma sono stati adottati adeguati protocolli per garantire la sicurezza e la privacy dei dati personali degli utenti. È importante continuare a monitorare l'utilizzo dell'app Immuni e adottare le necessarie misure di tutela dei dati personali degli utenti.[70]

[68] Art.5, par.1, lett.c) ed e) del Regolamento.

[69] Art.6, comma 2, lett.e), del d.l. n. 28/2020.

[70] Cfr.Ministero della Salute,*Valutazione d'impatto sulla protezione dei dati personali presentata dal Ministero della Salute relativa ai trattamenti effettuati nell'ambito del sistema di allerta Covid-19 denominato "Immuni"* , Nota sugli aspetti tecnologici [9357972], 2020, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9357972.

CONCLUSIONI

Dall'analisi condotta emerge l'importanza di adeguarsi costantemente all'evoluzione tecnologica per garantire la protezione dei dati personali degli utenti. In questo contesto, il Regolamento generale sulla protezione dei dati (GDPR) rappresenta un fondamentale quadro normativo per il trattamento dei dati personali degli utenti, delineando i ruoli delle entità coinvolte nella manipolazione di questi dati e fornendo i giusti principi per un trattamento lecito dei dati.

Con lo sviluppo di applicazioni mobili, la necessità di proteggere i dati personali degli utenti è diventata sempre più importante. A tal fine, il GDPR rappresenta un quadro normativo essenziale per la raccolta, il trattamento e la conservazione dei dati personali degli utenti. Nel presente elaborato, vengono fornite linee guida per lo sviluppo di applicazioni mobili che rispettino le leggi e le normative applicabili, tra cui il GDPR, la protezione dei diritti di proprietà intellettuale e le norme sulla concorrenza e il mercato. Il rispetto di queste normative è fondamentale per garantire la legalità e la sicurezza dell'applicazione.

Le tecnologie emergenti, come l'intelligenza artificiale, il cloud computing, l'Internet delle cose e la blockchain, stanno rapidamente cambiando il modo in cui le aziende raccolgono, utilizzano e conservano i dati, ma creano anche nuove sfide per quanto riguarda la conformità alle leggi sulla protezione dei dati personali e sulla privacy. È fondamentale monitorare costantemente l'evoluzione tecnologica e adeguarsi di conseguenza per garantire la protezione dei dati personali degli utenti.

L'analisi dell'App Immuni ha permesso di valutare il bilanciamento tra il diritto alla salute pubblica e il diritto alla riservatezza dei dati personali degli utenti. L'applicazione, sviluppata per contrastare l'emergenza sanitaria, ha mostrato come sia necessario tutelare la privacy degli utenti in ogni fase del trattamento dei dati personali.

In generale, l'elaborato ha evidenziato l'importanza di rispettare le norme e le leggi in vigore per garantire la legalità e la sicurezza di un'applicazione. In particolare, lo sviluppo di un'applicazione deve tenere in considerazione il rispetto della privacy degli utenti, che deve essere protetta in ogni fase del trattamento dei dati personali. Le tecnologie emergenti rappresentano una sfida per la conformità alle leggi sulla protezione dei dati personali e sulla privacy, ma è possibile affrontarle adeguandosi alle normative vigenti e monitorando costantemente l'evoluzione tecnologica.

BIBLIOGRAFIA

Baldassarre*, L 'App Immuni al banco di prova, tra rispetto della privacy e difesa della salute pubblica*, Roma, 2020.

Blandini, *Diritto dell'innovazione,* CEDAM, Milano,2022.

Cinque, *Privacy, Big-data e contact tracing: il delicato equilibrio fra diritto alla riservatezza ed esigenze di tutela della salute,* Roma,2020.

Coraggio, *Privacy e data Protection* 2022, IPSOA, Milano,2022.

Faini- Pietropaoli, *Scienza giuridica e tecnologie informatiche,* Giappichelli, Torino,2021.

Ferri, Diritto costituzionale e nuove tecnologie, Edizioni Scientifiche Italiane, Verona,2022.

Festa, *Ultimo capitolo della saga IMMUNI: l'App, autorizzata dal Garante, è finalmente negli store*, Milano, 2020.

Finocchiaro, *Diritto di internet,* Zanichelli, Bologna,2020.

Finocchiaro*, I contratti aventi ad oggetto il software*, Bologna,2014.

Iaselli, *I problemi giuridici che scaturiscono dallo sviluppo e dall'utilizzo delle applicazioni ne settore mobile sono fondamentalmente due: quello relativo al trattamento dei dati, ovvero della privacy e quello relativo alla qualificazione giuridica delle App*, Roma ,2015.

Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali, il Regolamento europeo 2016/679*, Giappichelli Editore, Torino, 2016.

Quarta - Smorto, Diritto *privato dei mercati digitali*, Firenze, 2020.

RODOTA', *Tecnologie e diritti*, Bologna ,1995.

STRUMENTI ESEGETICI

Gruppo di lavoro *ex* art. 29, Parere 1/2010

Gruppo di lavoro *ex* art. 29, parere 3/2010

SENTENZE E PROVVEDIMENTI

Provv. Garante Privacy, 09/12/1997, doc. web n. 30915

Provv. Garante Privacy, 01/06/2020, doc. web n. 9356568