Giuseppe Miceli
Monica Mandico
Elisabeta Cocolos

PRIVACY E GDPR

Trattamento dei dati personali per imprese, professionisti e amministrazioni

2ª Edizione completamente riveduta, aggiornata e arricchita
A cura di Giuseppe Miceli

LEGIS
GIURIDICA

LEGIS © è un marchio registrato **di Legislazione Tecnica S.r.L.**
00144 Roma, Via dell'Architettura 16

Finito di stampare nel mese di marzo 2024 da
LOGO SRL
Via Marco Polo, 8 - 35010 - Borgoricco (PD)

Servizio Clienti
Tel. 06/5921743 - Fax 06/5921068
servizio.clienti@legislazionetecnica.it

Portale informativo: www.legislazionetecnica.it
Shop: ltshop.legislazionetecnica.it

PREFAZIONI ALLA SECONDA EDIZIONE

Antonio Gerardo Giso

La leggenda vuole che, alla fine dell'Ottocento, l'Avvocato *Warren*, nell'accogliente città di Boston - stanco di leggere sul quotidiano locale i particolari della vita mondana della propria moglie e delle relazioni personali della propria figlia - decise di scrivere all'amico *Brandeis*, allora professore ad Harvard, per valutare il da farsi.

Da questa iniziativa nacque il saggio scritto, a quattro mani, dal titolo "*Right to privacy*" del 1890, che pose le basi per il riconoscimento, decenni a seguire, del diritto alla privacy, fondato per l'appunto sul "*Right to be alone*" e, ormai, entrato nel lessico comune.

Da allora di strada ne è stata fatta e, oggi, i dati sono sempre più considerati una tra le principali risorse del presente e del futuro. Non a caso, *Tim Berners-Lee*, l'inventore del *world wide web*, li ha definiti il petrolio del terzo millennio. L'Unione Europea sembra aver compreso, già da tempo, quanto possa essere importante fare una scelta di campo (e di mercato), con l'obiettivo di rendersi *leader* nel settore sia dal punto di vista tecnico che da quello del *design* normativo di tali applicazioni.

In principio fu il Regolamento (UE) 2016/679 (c.d. "*GDPR*") a rappresentare la prima vera rivoluzione in tema di regolazione del trattamento dei dati personali, con una applicazione trasversale in tutti gli Stati membri.

E, come spesso accade, mentre gli strumenti legislativi procedono a velocità di crociera, l'evoluzione tecnologica avanza a ritmi forsennati. A (soli) sei anni di distanza da quel fatidico 2018, anno di entrata in vigore del *GDPR*, in Europa oggi si discute dell'approvazione definitiva dell'*Artificial Intelligence Act* (c.d. "*AI Act*"). Il testo segna sicuramente un passo significativo nella regolamentazione dell'intelligenza artificiale, anche se non mancano preoccupazioni in termini di privacy e sicurezza informatica per le aziende.

Un'efficace regolamentazione della privacy rappresenta un punto chiave per consentire a tecnologie come l'intelligenza artificiale di aiutare a risolvere le più grandi sfide del mondo. Allo stesso tempo, è fondamentale riconoscere la necessità di un sistema legale per prevenire usi dannosi della tecnologia e per salvaguardare le informazioni personali.

La privacy, in quanto diritto fondamentale connaturato all'essere umano, merita una protezione efficace per consentire agli individui di fidarsi della tecnologia. È, infatti, essenziale trovare un equilibrio tra la capacità di effettuare un'analisi dei *Big Data* (e di conseguenza di abbracciare pienamente uno sviluppo etico dell'*AI*) e la tutela degli interessi e dei diritti in materia di *data protection*.

Questo volume, giunto alla seconda edizione, vuole essere un valido compagno di viaggio per chi (professionisti e aziende), quotidianamente, si trova a dover gestire il trattamento di dati, anche complessi e anche di nuova generazione.

Antonio Gerardo Giso
Avvocato in Roma
Lexant SBtA

Fernando De Santis

Interrogarsi sul concetto di privacy, alla soglia del quarto di secolo del terzo millennio, implica considerare una vasta gamma di questioni legate alla protezione dei dati personali, alla libertà individuale e alla sicurezza nell'era digitale. Oggi più che mai la privacy è diventata una questione preminente nella nostra vita, un fenomeno umano che prima lo Stato e poi l'Unione Europea hanno dovuto osservare, inseguire e infine regolare per garantire quello che è divenuto ormai il c.d. diritto alla privacy. Il percorso, usando un eufemismo, non è stato affatto semplice: anzi, scomodando il Poeta, il Legislatore ha dovuto attraversare proprio una *selva selvaggia e aspra e forte*.

Si può affermare che la normativizzazione del concetto di privacy, contrariamente alla visione hobbesiana dell'*homo homini lupus*, non ha un fondamento né contrattuale né utilitaristico, bensì personalistico, laddove l'uomo è considerato dotato di un significato e di un valore prevalente rispetto sia allo Stato sia a qualsiasi altra formazione sociale essendo queste ultime meri strumenti al soddisfacimento dei bisogni del singolo. E muovendo da tali premesse, è importante sottolineare che la persona umana occupa il ruolo primario nella positivizzazione della privacy all'interno dell'ordinamento giuridico e proprio tale ruolo caratterizza ogni persona per le libertà di cui dispone, per l'autonomia che esercita e l'autodeterminazione da cui è guidata.

Tali elaborazioni giuridiche non sono frutto di *autocombustione normativa spontanea*, ma derivano dagli studi tra il XIX e XX secolo: già John Stuart Mill difendeva il concetto di spazio privato come cruciale per la libertà individuale mentre l'evoluzione heideggeriana ha esplorato il concetto di "*essere con gli altri*" e l'importanza di avere uno spazio personale per riflettere e per essere autentico.

La privacy ormai permea e pervade la nostra vita quotidiana e racchiude in sé non solo la protezione dei dati personali, ma - con il sempre più repentino sviluppo delle ICT, ormai evolute in AI - riguarda le tecnologie al servizio della sorveglianza, i social media e le condivisioni delle informazioni, e interroga l'uomo su questioni di etica, autonomia e controllo: ecco che il presente volume vuole essere la bussola affinché il giurista, l'operatore di settore e finanche il cittadino possa affrontare in tranquillità la "*navigazione*" nel *mare magnum* della privacy.

Dott. Fernando De Santis

Samuele Tavagnacco

Il periodo che stiamo attraversando è caratterizzato da un processo di cambiamento continuo, un fenomeno intrinseco all'esistenza umana. Come affermato da Zygmunt Bauman nel libro "*Modernità liquida*", la realtà è in perenne trasformazione e il concetto di stabilità sembra perdere di significato di fronte al costante mutamento della società e delle sue strutture. Allo stesso modo, nel campo della privacy e della protezione dei dati, ci troviamo di fronte a una sfida analoga: come garantire sicurezza e riservatezza in un'era, quella digitale, nella quale ogni novità tecnologica potrebbe rendere obsoleto il quadro normativo vigente?

Come suggerito da Bauman, in questa post-modernità dobbiamo essere pronti a sostituire le vecchie soluzioni con le nuove, con la stessa fluidità con cui cambiano i contesti. Allo stesso modo le normative che governano la privacy e il trattamento dei dati personali, quali il GDPR, devono incorporare meccanismi di flessibilità e revisione continua. Le leggi sulla privacy non possono essere statiche ma devono essere pronte a modellarsi attorno alle ultime novità tecnologiche. Così facendo, sarà possibile non solo proteggere i dati personali, ma anche favorire l'innovazione responsabile, assicurandosi che la tecnologia operi nel rispetto della dignità umana e delle libertà individuali.

Il presente volume, dunque, attraverso un'analisi approfondita e accessibile, mira a fornire ai lettori gli strumenti necessari per comprendere e affrontare le complesse questioni legate alla protezione dei dati personali in un contesto sociale e tecnologico in costante mutamento. Nella società liquida di Bauman, la flessibilità e la capacità di adattamento non sono solo desiderabili ma fondamentali per la sopravvivenza umana. Parallelamente, il regolamento della privacy deve essere concepito per essere resiliente e capace di proteggere l'individuo senza ostacolarne l'innovazione.

Questa edizione del libro, aggiornata e arricchita, non solo fornisce una guida essenziale per navigare il complesso mare delle regolamentazioni attuali, ma invita anche a una riflessione più ampia sulla necessità di un approccio evolutivo alla protezione dei dati personali, in linea con i principi di una società che Bauman definirebbe liquida.

Samuele Tavagnacco
Studente LUISS
e Tirocinante al
Ministero dell'Economia e delle Finanze

INDICE

Si riporta di seguito l'indice della modulistica e della ulteriore documentazione varia fornita a corredo del volume, nell'Area download collegata allo stesso, accessibile con le modalità indicate nella seconda pagina di copertina.
La sigla accanto a ciascun elemento identifica il nome del file fornito in download; gli elementi contrassegnati con "D" sono unicamente disponibili in formato elettronico per il download.

MODULISTICA

DOCUMENTAZIONE VARIA

MODULISTICA E DOCUMENTAZIONE ESEMPLIFICATIVA IN LINGUA STRANIERA

NOTA PER IL DOWNLOAD

I materiali allegati al libro cartaceo sono disponibili nell'Area download collegata al volume, accessibile collegandosi all'indirizzo:

www.legislazionetecnica.it/download

ed inserendo il codice riportato nella seconda pagina di copertina dopo aver effettuato l'accesso con le proprie credenziali (chi non ne fosse in possesso dovrà preventivamente effettuare la registrazione gratuita al sito).

LEGIS
GIURIDICA

Pagine non disponibili in anteprima

2.4 NOMINA DEL RESPONSABILE DELLA PROTEZIONE DEI DATI - RPD (*DATA PROTECTION OFFICER* - DPO)

Il Regolamento europeo 2016/679 disciplina la figura del "*responsabile della protezione dei dati*" (articoli 37, 38, 39 e considerando 97), stabilendo che alcuni titolari e responsabili del trattamento sono tenuti a nominare un RPD (responsabile protezione dati) [28] o DPO (*Data Protection Officer*). Ciò vale per tutte le autorità pubbliche (eccetto i tribunali) e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali. Anche quando la nomina non è obbligatoria, l'eventuale designazione, su base volontaria, di un RPD è fortemente consigliata dalle Linee guida del Gruppo Articolo 29, essendo una figura professionale utile, nell'ambito del presidio del rischio, con l'aggiunta di competenze specialistiche. Se si procede alla nomina di un RPD su base volontaria, troveranno applicazione tutti i requisiti di cui agli articoli 37-39 per quanto concerne la nomina stessa, lo *status* e i compiti del RPD esattamente come nel caso di una nomina obbligatoria. Nulla osta a che un'azienda o un ente, quando non sia soggetta all'obbligo di designare un RPD e non intenda procedere a tale designazione su base volontaria, ricorra comunque a personale o consulenti esterni incaricati di

istituzionali, e pertanto non possono essere utilizzati per il perseguimento di altre finalità incompatibili, come appunto la propaganda elettorale; (ii) i partiti, le liste o i singoli candidati non possono utilizzare indirizzi di posta elettronica senza il consenso specifico e informato dei destinatari. Consenso che, nel caso in esame, non risultava essere stato acquisito, né i destinatari risultavano essere stati informati sull'uso che veniva fatto dei loro dati". Per maggiori informazioni sugli interventi più significativi compiuti dall'Autorità Garante in tema di Internet, nuove tecnologie e nuove forme di comunicazione elettronica, si veda il seguente link: *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5047936#1*.

[28] WP29, *Linee guida sui responsabili della protezione dei dati*, emanate il 13/12/2016 nella versione emendata e adottata in data 05/04/2017: "*La nomina di un RPD è obbligatoria anche con riguardo alle autorità competenti di cui all'articolo 32 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119, 4.5.2016), alla luce della normativa nazionale di recepimento. Le presenti linee guida guardano con particolare attenzione alla figura del RPD come prevista dal RGPD, ma le indicazioni in esse formulate valgono anche per i RPD previsti dalla direttiva 2016/680 con riferimento alle disposizioni di carattere analogo contenute nei due strumenti. 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 (GU L 281, 23.11.95)*".

incombenze relative alla protezione dei dati personali. In tal caso è fondamentale garantire che non vi siano ambiguità in termini di denominazione, status e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne (con l'autorità di controllo, gli interessati, i soggetti esterni in genere), queste figure o consulenti non siano indicati con la denominazione di "*responsabile della protezione dei dati*" [29].
Invero la figura del RPD non costituisce una novità assoluta. La Direttiva 95/46/CE non prevedeva alcun obbligo di nomina di un RPD, ma in alcuni Stati membri questa è divenuta una prassi nel corso degli anni.
Ancor prima dell'adozione del GDPR, il Gruppo Articolo 29 ha sostenuto che questa figura rappresenta un elemento fondante ai fini della responsabilizzazione, e che la nomina del RPD possa facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese. Oltre a favorire l'osservanza attraverso strumenti di *accountability* (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati), i RPD fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente.
In base all'articolo 37, par. 1, del GDPR, la nomina di un RPD è obbligatoria in tre casi specifici [30]:

a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico [31], con l'eccezione delle autorità giudiziarie nell'esercizio

[29] Queste considerazioni valgono anche per i *Chief Privacy Officers* (CPO) o altri professionisti in materia di privacy già operanti presso alcune aziende, che non sempre e non necessariamente si conformano ai requisiti fissati nel Regolamento per quanto riguarda, per esempio, le risorse disponibili o le salvaguardie della loro indipendenza e che, in tal caso, non possono essere considerati e denominati "*RPD*".

[30] Si osservi che, in base all'articolo 37, par. 4, il diritto dell'Unione o dello Stato membro può prevedere casi ulteriori di nomina obbligatoria di un RPD.

[31] Nel Regolamento non si rinviene alcuna definizione di "*autorità pubblica*" o di "*organismo pubblico*". Il Gruppo di lavoro Articolo 29 ritiene che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico. In questi casi la nomina di un RPD è obbligatoria. Lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri non pertengono esclusivamente alle autorità pubbliche e agli organismi pubblici, potendo riferirsi anche ad altre persone fisiche o giuridiche, di diritto pubblico o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di disciplina professionale. In tutti questi casi la situazione in cui versano gli interessati è probabilmente molto simile a quella in cui il trattamento è svolto da un'autorità pubblica o da un organismo pubblico. Più in particolare, i trattamenti perseguono finalità simili e spesso il singolo ha, in modo analogo, un margine esiguo o nullo rispetto alla possibilità di decidere se e come possano essere

delle funzioni giurisdizionali (vedi articolo 32 della Direttiva UE 2016/680);

b) se le "*attività principali*" del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
c) se le "*attività principali*" del titolare o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati [32] o di dati personali relativi a condanne penali e reati [33].

Il RPD viene designato, su base obbligatoria o meno, per tutti i trattamenti svolti dal titolare del trattamento o dal responsabile del trattamento.

2.4.1 Il concetto di "*attività principali*"

In merito al significato di "*attività principali*" cui l'articolo 37, par. 1, lettere *b)* e *c)*, del GDPR fa riferimento ("*attività principali del titolare del trattamento o del responsabile del trattamento*"), si richiama il considerando 97, in virtù del quale le attività principali di un titolare del trattamento "*riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria*". Con "*attività principali*" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento. Tuttavia, l'espressione "*attività principali*" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento. Per esempio, l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un RPD.

---

trattati i propri dati personali; pertanto, è verosimile che sia necessaria l'ulteriore tutela offerta dalla nomina di un RPD.

[32] Ai sensi dell'articolo 9, si tratta dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose, o l'appartenenza sindacale, oltre al trattamento di dati genetici, dati biometrici al fine dell'identificazione univoca di una persona fisica, e di dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona fisica.

[33] Articolo 10.

LEGIS
GIURIDICA

Pagine non disponibili in anteprima

QUADRO SANZIONATORIO

di Giuseppe Miceli

1 SANZIONI DI NATURA AMMINISTRATIVA

Il nuovo quadro sanzionatorio previsto dal Regolamento UE 2016/679 si fonda sul principio in virtù del quale ogni sanzione dovrà essere applicata in base alla gravità, alla natura e alla durata della violazione al GDPR, nonché in base al numero di soggetti coinvolti e al carattere doloso o colposo della violazione contestata.
Le sanzioni amministrative pecuniarie riportate di seguito possono essere integrative, oppure completamente sostitutive delle sanzioni correttive indicate nell'elenco successivo; si distinguono in *sanzioni di carattere economico* e *sanzioni correttive*.

1.1 Sanzioni di carattere economico

Tali sanzioni si applicano in caso di:

- inosservanza degli obblighi del titolare e del responsabile del trattamento; inosservanza degli obblighi dell'organismo di certificazione; inosservanza degli obblighi dell'organismo di controllo: fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato annuo mondiale dell'esercizio precedente;
- inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati; inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali; inosservanza di un ordine di limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo: fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente;
- inosservanza di un ordine correttivo dell'autorità di controllo: fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente.

1.2 Sanzioni correttive

Le sanzioni correttive sono connesse ai poteri dell'autorità di controllo. Esse consistono nel:

- rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare il GDPR;
- rivolgere ammonimenti al titolare del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del GDPR;
- ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti;

LEGIS
GIURIDICA

Pagine non disponibili in anteprima

FOCUS - ATTIVITÀ DI ISPEZIONE IN MATERIA DI PRIVACY

di Giuseppe Miceli

Le ispezioni privacy: operatività e consigli utili

Dalla Relazione annuale presentata dal Garante privacy lo scorso 06/07/2023 emerge che il 2022 ha visto una serie di interventi centrati sulle grandi questioni legate alla tutela dei diritti fondamentali delle persone nel mondo digitale: in particolare, le implicazioni etiche della tecnologia; l'economia fondata sui dati; le grandi piattaforme e la tutela dei minori, i sistemi di *age verification*; i *big data*; l'intelligenza artificiale generativa, il Metaverso e le problematiche poste dagli algoritmi; gli scenari tracciati dalle neuroscienze; la sicurezza dei sistemi e la protezione dello spazio cibernetico; la monetizzazione delle informazioni personali; i fenomeni del *revenge porn*, del cyberbullismo, dello *sharenting*, del *social scoring*.

Particolare attenzione è stata posta dal Garante privacy all'uso dei dati biometrici e al diffondersi di sistemi di **riconoscimento facciale**. In questo ambito, in particolare, l'Autorità ha sanzionato per 20 milioni di euro la società statunitense ***Clearview***, vietando l'uso dei dati biometrici e il monitoraggio degli italiani.

Sul fronte della **tutela online dei minori**, nel corso del 2022 è proseguita l'azione di vigilanza sull'età di iscrizione ai social, anche attraverso sistemi di *age verification*. In questa direzione si muove il tavolo di lavoro istituito con il recente protocollo d'intesa tra Garante e AGCOM.

Inoltre, dopo l'altolà del Garante, **Tik Tok** ha sospeso l'invio di pubblicità personalizzata basata sul legittimo interesse. Oltre ad una base giuridica inadeguata vi erano, infatti, seri rischi che la pubblicità potesse raggiungere i giovanissimi con contenuti non appropriati.

Sul fronte della **cybersecurity**, l'Autorità ha avviato la collaborazione con la Agenzia nazionale per la sicurezza con la quale è stato firmato un protocollo di intesa.

Come si può leggere in "*Le cifre dell'attività del Garante privacy - Annualità 2022*" (Appendice), le **ispezioni** effettuate nel 2022 sono state **140**, quasi triplicate rispetto a quelle dell'anno precedente in cui ancora si subiva l'impatto dell'emergenza pandemica. Gli accertamenti svolti, anche con il contributo del Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di Finanza, hanno riguardato diversi settori, sia nell'ambito pubblico che privato: in particolare, telemarketing, cloud pubblico, siti web ed uso dei cookie, videosorveglianza, anche sul posto di lavoro. Sono state effettuate effettuate verifiche periodiche al VIS (*Visa Information System*), il sistema sui visti d'ingresso nello spazio Schengen.

APPROFONDIMENTO

Deve tenersi conto che le attività ispettive e di controllo in materia di privacy, così come previste e disciplinate dal GDPR, hanno abbandonato l'obsoleto carattere di "*staticità*" tipizzato in una mera spunta della c.d. *"check-list privacy"* e hanno assunto il carattere della "*dinamicità*" che contraddistingue la ricerca continua e proattiva di *compliance* rispetto al GDPR, alla normativa nazionale e ai provvedimenti delle Autorità di controllo.
In pratica: in fase di attività ispettiva potrà anche emergere la mancata adozione di una "*misura*" di protezione dei dati personali (per esempio, la nomina del DPO); tuttavia, non automaticamente ne scaturiranno la contestazione e la sanzione.
Determinante sarà - sulla base del principio di *accountability* - la condotta del titolare del trattamento, sottoposto al controllo, che potrà dare dimostrazione (comprovare) sulla base della ricostruzione logico-giuridica che non si tratti di un mancato adempimento, bensì del legittimo risultato di una attenta valutazione.
Dirimente, pertanto, in fase di ispezione, è la capacità del titolare o responsabile del trattamento di saper dare conto - in maniera *accountability* - delle scelte operate e delle decisioni applicate.

I poteri ispettivi del Garante consentono l'accesso a banche dati, archivi nei luoghi in cui si svolge il trattamento o nei quali è necessario effettuare verifiche utili al controllo del rispetto della normativa sul trattamento dei dati personali. Inoltre, il Garante può chiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile nominati, all'interessato o anche a terzi di fornire informazioni o di esibire documenti anche in relazione a banche dati.
Ai sensi dell'art. 158, comma 4, del Codice privacy, se l'ispezione disposta dal Garante deve svolgersi in un'abitazione o un altro luogo di dimora privata è necessario "*l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento*" [1].
L'accertamento non può essere iniziato prima delle ore sette e dopo le ore venti salvo diversa disposizione del decreto del presidente del Tribunale.
In caso di rifiuto, gli accertamenti sono comunque eseguiti e le spese ove occorrenti sono poste a carico del titolare con il provvedimento che definisce il procedimento.

[1] In quest'ultimo caso dovrà essere rilasciata una copia del provvedimento di autorizzazione del Tribunale alla parte.