Gianluca Amarù,
Alessandra Fava, Marco Fossi

La privacy dei dati digitali

Consigli pratici sugli archivi informatizzati, la nuova figura del responsabile dei documenti digitali, il consenso, il data breach e l'e-commerce

FrancoAngeli

MANAGEMENT

TOOLS

FrancoAngeli
Edizioni La passione per le conoscenze

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con **Adobe Acrobat Reader**

La versione completa dell'e-book (a pagamento) è leggibile **con Adobe Digital Editions**.

Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta **cliccando qui** le nostre F.A.Q.

MANAGEMENT TOOLS

Visioni, esperienze, metodologie per potenziare competenze e capacità: proprie e dei collaboratori

---

Management Tools offre a tutti i professional (e agli imprenditori) testi precisi, puntuali, agili e innovativi. Scritti appositamente da consulenti qualificati, i volumi affrontano tutte le aree e i temi di rilievo per valorizzare le competenze e indirizzare al successo le organizzazioni.

Gianluca Amarù,
Alessandra Fava, Marco Fossi

La privacy dei dati digitali

Consigli pratici sugli archivi informatizzati, la nuova figura del responsabile dei documenti digitali, il consenso, il data breach e l'e-commerce

FrancoAngeli
TOOLS

Indice

Introduzione

Il nostro libro vuole essere uno strumento di lavoro. Innanzitutto per le imprese che oggi si trovano ad approcciare mercati di riferimento con modalità sempre più digitali. In materia di privacy, anche a causa delle sanzioni amministrative che le Autorità possono comminare, i Titolari oggi devono essere informati, pro-attivi e in linea con le tendenze normative e con le nuove sensibilità degli attori presenti sul mercato. Bisogna infatti considerare che la digitalizzazione degli archivi di dati personali comporta le stesse regole di quelli cartacei, semmai rafforzate dal punto di vista della sicurezza logico-informatica. Ancora una volta si conferma il fatto che l'impegno per raggiungere la piena compliance debba essere continuo per essere al passo con la velocità con cui mutano e impattano le tecnologie sulla vita dei cittadini, delle imprese e sulle relazioni tra loro.

Il volume è anche un manuale per i DPO, Data Protection Officer, che per fornire una consulenza adeguata, che siano esterni o interni all'azienda, sono tenuti a un aggiornamento continuo. Qui troveranno come affrontare il tema del cloud, le Linee Guida AgID e altre novità.

Siamo convinti che anche il cittadino, interessato ai temi di tutela dei dati e della privacy in generale, possa trovare nel nostro libro spunti di riflessione.

1 Come costruire un sito di e-commerce compliant. Come gestire i cookie sia sui siti tradizionali che su quelli di e-commerce, secondo le norme vigenti; i comportamenti opachi (*dark patterns*) secondo le ultime Linee Guida EDPB

1.1. Il Far West digitale sta finendo

Una cattiva gestione dei cookie e informative carenti, confuse e poco trasparenti sul sito aziendale o su quello di e-commerce, sono scelte che potrebbero comportare delle sanzioni. Oggi non è più possibile avere un comportamento opaco ed eludere le nuove normative sulla concorrenza: il nuovo Regolamento UE sull'e-commerce è entrato in vigore a luglio 2020 e così il Digital Market Act (DMA), ovvero il Regolamento 2022/1925, è entrato in vigore nel novembre 2022 con applicazione in tutti i Paesi UE dal 2 maggio 2023. Il DMA riguarda le mega aziende globali del web, ma non solo. Inoltre è stato pubblicato il Digital Services Act che regolamenta i prestatori di servizi online. Quindi tutte le imprese che hanno un sito internet, tutti quelli che fanno e-commerce, le piattaforme di marketplace e comunque tutti quelli che comunicano attraverso il web con una rete di clienti, quindi anche i motori di ricerca, devono per *privacy by design* stabilire le regole e costruire dei sistemi privacy a norma. Il Far West digitale sta finendo. Dietro a tutto c'è anche la consapevolezza che le continue innovazioni tecnologiche trovano nuove vie per raccogliere dati personali sotto traccia, quindi i regolatori europei sono determinati a combattere la microprofilazione e stanno affinando nuovi strumenti legislativi.

Il GDPR, il Regolamento europeo 2016/679, resta un punto di riferimento imprescindibile, ma a questo si aggiungono le Linee Guida dell'EDPB, il Board Europeo e le espressioni del Garante italiano, ad esempio in materia di cookie (2014 e 2018). Insomma la microprofilazione non sembra aver molto futuro.

1.2. Che cosa sono i cookie e perché sono importanti

Per costruire un sito compliant prima di tutto l'utente/Interessato deve dare il consenso o meno a cookie di profilazione oppure essere libero di usare i soli cookie tecnici, propedeutici alla navigazione sul sito. La scelta, per essere libera, non deve impedire la navigazione sul sito nel caso l'Interessato scelga "prosegui senza accettare" o "rifiuta tutto" o "usa solo cookie tecnici". Purtroppo alcuni editori italiani ed europei hanno scelto di imporre "accetta tutti i cookie" a chi vuole navigare gratuitamente su un sito di informazioni oppure "Rifiuta e abbonati". Mentre scriviamo, il Garante italiano ha aperto un'inchiesta su questo comportamento.

Ma procediamo con ordine. I cookie non sono biscottini, anche se così li hanno chiamati scherzosamente i primi programmatori. Sono dei piccoli file di testo che il sito visitato manda al terminale del visitatore. Se il visitatore ritorna in quel sito, i cookie vengono ritrasmessi. Prima di tutto distinguiamo tra **cookie tecnici e cookie di profilazione**.

I tecnici o essenziali, detti anche "strettamente necessari" o di funzionalità, sono quelli usati per effettuare una trasmissione o una comunicazione su una rete elettronica nella misura strettamente necessaria al fornitore di quel servizio. Insomma, per farla brev,e servono per navigare in un sito. Infatti a volte nei siti ci sono elementi che arrivano da server diversi da quello del sito visitato, ad esempio immagini, cartine o link ad altri siti. Inoltre i cookie tecnici raccolgono dei dati aggregati sui naviganti che possono essere utili per il gestore del sito.

I cookie tecnici a loro volta possono essere divisi in **cookie di navigazione di sessione** o **cookie di analisi o analitici**. I primi garantiscono la navigazione e l'utilizzazione del sito web, ad esempio si attivano per permettere a chi naviga di fare un acquisto online oppure di accedere a servizi. I cookie di analisi o analitici rientrano sempre nella categoria dei tecnici se sono utilizzati solo dal gestore del sito e non da soggetti terzi, e dovrebbero servire solo per agevolare la navigazione nel sito e raccogliere dati in forma aggregata dei navigatori.

I cookie tecnici o indispensabili quindi non sono strumenti di tracciamento o profilazione.

I **cookie di profilazione**, invece, hanno il fine di profilare l'Interessato in modo da carpirne gusti, abitudini, zona di residenza, hobby, composizione della famiglia, predisposizione agli acquisti, capacità di spesa. Tutti questi dati servono al gestore del sito per indirizzare alle persone comunicazioni di pubblicità di oggetti, opportunità, servizi che potrebbero essere interessati ad acquistare, utilizzare o che vengono già usati dal cliente, in base alle preferenze date in passato, durante la sua navigazione web. Questi dati vengono anche venduti a terzi. Quindi i cookie di profilazione

sono approntati per fornire più dati possibili al gestore o ad altri soggetti rispetto al navigante. I dati vengono raccolti, analizzati e riutilizzati **a fini di marketing** e, con l'evolversi delle tecnologie, si prefiggono persino di influenzare le scelte del singolo, fino a predire il suo comportamento. In linea astratta sono utili al gestore e alle parti terze anche per lungo tempo, ma le disposizioni di legge prevedono limitazioni temporali e sono vincolati alla richiesta obbligatoria di consenso da parte del cittadino/Interessato. Dobbiamo infatti tener conto del fatto che i coockie di profilazione possono provenire sia dal Titolare della pagina web, sia da soggetti terzi. E quando parliamo di parti terze, il Titolare del sito potrebbe non conoscere le finalità perseguite dai soggetti che ospita e non essere in grado di controllarne l'operato. Inoltre i dati pervenuti a terze parti potrebbero essere ceduti o modificati da altri soggetti. Quindi per il gestore del sito risulta difficile tenere traccia di queste evenienze e dare un'informativa su finalità ignote o perseguite da altri soggetti, e questo aumenta la "rischiosità" in termini di tutela dei dati personali. Perciò sono stati messi tanti paletti sui cookie di profilazione.

1.3. La normativa sui cookie

Da anni le Autorità Garanti della privacy si interrogano sulla tutela dei dati personali dei cittadini anche online, e da tempo cercano di mettere dei freni e normare gli aspetti più rischiosi. Il Garante italiano è tra quelli che si è attivato prima, anche grazie alla giurisprudenza italiana e alle normative sulla privacy messe in atto dagli anni Novanta, quindi agli albori della rete e del web. Anche per i cookie l'Italia è tra i primi Paesi che ha tentato di fermare il Far West totale della prima ora. Già nel 2014 il Garante per la privacy emise un primo provvedimento **(n. 229 dell'8 maggio del 2014)** dal titolo *Individuazione delle modalità semplificate per informative e per l'acquisizione del consenso per l'utilizzo dei cookie,* pubblicato sulla Gazzetta Ufficiale n. 126 del 3 giugno 2014. Il provvedimento prevede che il Titolare del trattamento faccia attenzione alla collocazione del fornitore della piattaforma web. I cookie qui vengono chiamati "file di testo di minuscole dimensioni che le web page visitate inviano al terminale": per terminale s'intende un pc, uno smartphone, un tablet di proprietà dell'utente. In caso di nuova consultazione possono essere ritrasmessi al sito. Ciò avviene in maniera del tutto automatica e non direttamente intellegibile da parte dell'utente. Quindi si ricevono cookie anche da parte di server differenti da quello del sito visitato. I cookie possono essere utilizzati per l'autenticazione informatica dell'utente, ad esempio, quando accede alla posta elettronica, per il monitoraggio di sessioni di connessioni, per l'esame di eventuali aggiornamenti e

software utilizzati per aggiornamenti o altro. Quel che ci interessa maggiormente è che in questo provvedimento del 2014 il Garante disse che i cookie sono da considerarsi dati personali e che già allora venivano individuate due macro-categorie di cookie: i cookie tecnici e quelli di profilazione. Inoltre il Provvedimento 2014 presentava la novità della scomparsa **dell'obbligo di notificazione del trattamento al Garante**. Infatti, secondo la precedente disciplina (legge n. 196 del 2003) chi utilizzava cookie di profilazione – in quando file caratterizzati dalla permanenza nel tempo di abitudini, scelte di consumo dell'utente e capacità di spesa – obbligava il Titolare del sito alla notificazione al Garante.

Bisogna tenere presente che anche il Regolamento GDPR 2016 entrato in vigore a maggio 2018, parla direttamente di cookie solo nel Considerando 30: "*Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP,* ***marcatori temporanei (cookie)*** *o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare, se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle*".

E all'art. 3 del GDPR, si accenna al "monitoraggio del comportamento" (degli interessati) e si dispone che l'utilizzo dei *cookie* sia possibile solo previa **informativa** resa all'Interessato e previa acquisizione di **consenso** da parte dello stesso.

Quindi anche per i cookie di profilazione serve il consenso, facendo riferimento all'art. 4, punto 11 e al Considerando 32 laddove si parla del fatto che l'Interessato deve poter manifestare un'"**intenzione libera, specifica, informata e inequivocabile**", "non dovrebbe configurare consenso il silenzio, l'inattività o la preselezione di caselle" e infine "se il consenso è richiesto attraverso mezzi elettronici la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso".

Allo stesso modo l'art. 4 al punto 11 parla di "dichiarazione o azione positiva, inequivocabile" di consenso. Anche il Garante italiano, commentando le Linee Guida EDPB e poi emanandone, come vedremo, di più stringenti, sottolinea quell'"inequivocabile", che vuol dire a scanso di equivoci. Insomma l'Interessato, l'internauta, deve consapevolmente scegliere di essere tracciato o meno.

Quindi il consenso deve essere un elemento previsto in fase progettuale nelle pagine web e costruito secondo il principio della *privacy by design*, ovvero in fase di progettazione del sito. Tale consenso va monitorato continuamente e deve essere revocabile in toto o in parte, per la *privacy by default.*

Nell'**allegato 1 al provvedimento 467 dell'11 ottobre 2018** pubblicato sulla Gazzetta ufficiale col titolo *Elenco delle tipologie dei trattamenti soggetti al meccanismo di coerenza da sottoporre alla Valutazione d'impatto*, il Garante per la Protezione dei Dati Personali ha individuato alcune tipologie di trattamento per i quali è obbligatoria una Dpia, vale a dire una Valutazione d'impatto sulla protezione dei dati personali trattati. Tra queste tipologie troviamo, al numero 3, i trattamenti che prevedono l'utilizzo sistematico di dati per l'osservazione, il monitoraggio e il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuata online, o attraverso app, o attraverso trattamenti identificativi univoci, in grado di identificare gli utenti di servizi della società dell'informazione, inclusi i servizi web, la tv interattiva rispetto alle abitudini d'uso e i dati di visione per tempi prolungati. Rientrano nel novero anche il trattamento di metadati effettuati non solo per la profilazione, ma più in generale per ragioni organizzative, previsione di badget, upgrade tecnologico e miglioramento delle reti, offerte di servizi anti-frode, spamming, servizi di sicurezza etc. Quindi rientra nell'**obbligo della Dpia anche il sito web dell'azienda di un Titolare**. E questo anche nell'ipotesi in cui scelga in fase di progettazione di escludere l'uso di cookie di profilazione.

A queste normative si aggiungono le Linee Guida del WP29 adottate il 10 aprile 2018, ratificate dal Comitato europeo per la Protezione dei dati personali (di seguito, EDPB) il 25 maggio 2018, poi sostituite e integrate dalle *Guidelines 05/2020 on consent under Regulation 2016/679* adottate il 4 maggio 2020 dal Comitato europeo EDPB.

1.4. Le Linee Guida dell'EDPB

Infatti il 4 maggio 2020, anche l'EDPB (European Data Protection Board), detto anche Comitato europeo per la Protezione dei dati, si è espresso con delle Linee Guida relative al consenso e ai cookie: *Guidelines 05/2020 on consent under Regulation 2016/679*. Prima di tutto le Linee Guida sottolineano che il consenso deve essere specifico, informato, inequivocabile e revocabile. L'EDPB rileva che per valutare se il consenso sia stato prestato liberamente bisogna attenersi all'articolo 7, paragrafo 4, del Regolamento, quindi è ILLECITO "inserire" il consenso nell'accettazione delle condizioni generali di contratto/servizio o «subordinare» la fornitura di un contratto o servizio alla richiesta di consenso al trattamento di dati personali che non sia necessario per l'esecuzione del contratto o servizio. A questo discorso segue anche l'esempio di un'app da scaricare per ritoccare le foto: la fornitura dell'app gratuita non può essere condizionata al via libera da parte dell'utente al rilevamento della sua posizione GPS, perché

in tal modo il consenso sarebbe vincolato alla concessione di un dato personale.

Così le Autorità pubbliche, avendo spesso un ruolo sbilanciato rispetto al cittadino, non devono eccedere nella richiesta di consenso. L'EDPB in questo caso fa l'esempio di un cantiere comunale e di una mailing list per avere informazioni sull'andamento dei lavori: è chiaro che presteranno consenso solo coloro che vorranno ricevere le informazioni, ma non avrà nessun danno chi non acconsentirà a fornire dati personali o la propria mail all'amministrazione. Quindi non ci devono essere danni né favori, né per aderenti, né per chi si rifiuta di fornire i propri dati.

Al paragrafo 25 dedicato alla "Condizionalità", si legge infatti che "*per valutare se il consenso sia stato prestato liberamente è di rilievo l'articolo 7, paragrafo 4, del Regolamento*", vale a dire "*Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*". Cfr. anche il Considerando 43 dello stesso Regolamento, che afferma: "*[...] Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione*".

Insomma tutto l'impianto dell'EDPB è che "è essenziale che l'Interessato abbia il controllo dei propri dati". E se si dà il via a due trattamenti ci vogliono due consensi separati.

Nei paragrafi centrali delle Linee Guida si entra in *media res*. Al paragrafo 39 si parla dei *cookie wall*: "*Affinché il consenso sia prestato liberamente, l'accesso ai servizi e alle funzionalità non deve essere subordinato al consenso dell'utente alla memorizzazione di informazioni o all'ottenimento dell'accesso a informazioni già memorizzate nell'apparecchiatura terminale dell'utente (i cosiddetti 'cookie wall')*".

Segue l'esempio di un sito al quale il lettore non può accedere se non dice sì a tutti i cookie. Ovviamente questo è un comportamento non appropriato e contro la legge perché il provider/titolare vincolerebbe il consenso ai cookie alla fornitura di un servizio. Così al paragrafo 40 delle Guidelines si indica il caso del web provider che blocchi la visibilità di un certo contenuto qualora non sia stato prestato il consenso ai cookie. Inutile osservare come in questo caso il consenso eventualmente prestato risulti essere "viziato" e quindi invalido.

Il ragionamento del Board Europeo EDPB è che se il *cookie wall* è composto da cookie che permettono l'accesso e/o la navigazione su una pagina

web, gli stessi devono essere accettati dall'utente. Se l'utente presta il consenso spesso può autorizzare senza avvedersene anche il tracciamento dei propri dati ed una profilazione realizzata in maniera nascosta ed illecita rispetto ai principi enunciati dal GDPR.

1.5. Il consenso sul web

Vediamo ora qual è la formula lecita di richiesta del consenso online. Le Linee Guida dell'EDPB hanno espresso chiaramente il **principio della granularità**: "*l'Interessato dovrebbe essere libero di scegliere quali finalità accettare anziché dover acconsentire a un insieme di finalità*" e quindi deve poter fornire "*un consenso separato ai distinti trattamenti dei dati personali*".

Al paragrafo 44 si legge che "*Se il Titolare del trattamento ha riunito diverse finalità di trattamento e non ha chiesto il consenso separato per ciascuna di esse, non c'è libertà*". Ad esempio non è corretto che un fornitore di un servizio chieda contemporaneamente e con un solo documento il consenso per il trattamento dei dati ai fini di marketing e anche la cessione dei dati ad altre società del gruppo. Le due richieste devono essere divise.

Nel consenso deve essere chiaramente espresso: chi è Titolare, la finalità, quali tipi di dati vengono raccolti, la possibilità di revoca, eventuale processo automatico di profilazione, informazioni sui rischi di trasferimento dei dati e, se ci sono più titolari del trattamento, vanno tutti indicati. Ovviamente il linguaggio deve essere chiaro, semplice, intellegibile. Un altro aspetto importantissimo è il **principio di revocabilità del consenso**. La revocabilità deve essere possibile senza danni, costi o svantaggi per l'utente. Insomma il consenso è fornito liberamente se "*il servizio non viene diminuito a scapito dell'utente*".

Al paragrafo 84 si parla anche delle modalità di consultazione del sito e si ribadisce che lo ***scrolling*** (tradotto come "prosecuzione dell'uso normale del sito web") non può equivalere a un consenso:

Il Titolare del trattamento dovrebbe progettare meccanismi di consenso che operano in maniera chiara per gli interessati. Il Titolare del trattamento deve evitare ambiguità e garantire che l'azione con cui viene espresso il consenso possa essere distinta da altre azioni. La semplice prosecuzione dell'uso normale di un sito web non è pertanto un comportamento dal quale si può dedurre una manifestazione di volontà dell'Interessato a prestare il consenso a un trattamento proposto.

Già le Linee Guida del WP29 (che è un po' antesignano dell'EDPB) nel 2018 avevano previsto che:

lo scrolling non costituisse un'azione chiara e positiva in considerazione del fatto che l'avviso che continuare a scorrere il sito costituirà un'espressione di consenso può essere difficile da distinguere e/o può essere trascurato inavvertitamente quando l'Interessato scorre rapidamente grandi quantità di testo; inoltre tali azioni non sono sufficientemente inequivocabili.

Il WP29 parlava espressamente dello *scrolling* perché nel frattempo, dovendo in qualche modo regolamentare il consenso ai cookie di profilazione, molti siti erano ricorsi a degli escamotage. Ad esempio, bastava che il lettore scorresse la pagina web per far desumere che quel gesto fosse equiparabile a un consenso, ovvero a un via libera ai cookie di vario tipo. Insomma il "leggere" la pagina equivaleva a fornire il consenso, anche laddove di consenso non si parlava esplicitamente da nessuna parte. Insomma l'azione positiva deve essere inequivocabile. Quindi il Titolare non può approfittare del fatto che l'Interessato è costretto a passare varie pagine, magari è distratto e clicca sì in modo poco consapevole.

Quindi è logico come il Comitato europeo EDPB – composto dal responsabile di un'Autorità di controllo di ciascun Stato membro e presieduto dal Garante Europeo della Protezione dei Dati – abbia focalizzato la sua attenzione non già sui cookie tecnici che sono indispensabili per la navigazione e l'autenticazione, ma sui cookie di terze parti, soprattutto su quelli di profilazione. Infatti, come abbiamo spiegato prima, mentre i cookie tecnici supportano la navigazione e raccolgono dati non troppo specifici rispetto al singolo navigante, quelli a uso marketing/profilazione possono "tracciare" e tenere a memoria comportamenti, abitudini, preferenze, interessi e scelte dell'utente anche al fine di proporre una pubblicità mirata. Insomma i dati personali raccolti vengono chiaramente utilizzati a fini pubblicitari e di creazione di cluster. Quindi ai sensi del Regolamento Europeo tali trattamenti necessitano di consenso ed è da rilevare che sono soggetti anche alle regole sul tempo massimo in cui possono essere trattati tali dati, la cosiddetta Data Retention.

A fronte di questo, anche il Comitato europeo per la Protezione dei Dati (EDPB) nel 2020 ha scritto che lo ***scrolling*** (il far scorrere la pagina) non può essere considerato espressione di un consenso, perché non costituisce un'azione sufficientemente chiara e positiva:

azioni come scorrere o sfogliare una pagina web o come altra attività analoga dell'utente, non potranno in qualsivoglia modo soddisfare il requisito dell'azione chiara e positiva: dette azioni si distinguono ben difficilmente da altre attività o interazioni dell'utente e perciò con esse non sarà possibile stabilire che sia stato ottenuto un consenso privo di ambiguità.

Da ciò è evidente che avvisi come "*continuare a navigare sul sito costituirà un'espressione di consenso*" non costituiscono certo una valida infor-

mativa all'utente. Anche perché l'avviso o il pop possono essere difficili da distinguere da altre prescrizioni presenti sulla pagina, oppure possono essere trascurati inavvertitamente, se l'Interessato scorre rapidamente grandi quantità di testo. *"Per di più* – scrive l'EDPB – *in un caso come questo, sarebbe difficile offrire all'utente* ***la possibilità di revocare il consenso*** *in un modo che fosse altrettanto semplice come averlo prestato"*.

Piuttosto il consenso può essere fornito **online** in più modi:

Nel contesto digitale od online, l'Interessato può emettere la dichiarazione richiesta compilando un modulo elettronico, inviando un'e-mail, caricando un documento scansionato con la propria firma oppure utilizzando una firma elettronica. In teoria, anche l'uso di dichiarazioni verbali può essere sufficientemente specifico per ottenere un consenso esplicito valido; tuttavia può essere difficile per il Titolare del trattamento dimostrare che tutte le condizioni per la validità del consenso esplicito siano state soddisfatte quando la dichiarazione è stata registrata.

Come troviamo anche in altre norme, il consenso verbale è lecito, ma è difficile da dimostrare a meno che il Titolare non tenga un database vocale. Quindi in generale è fortemente caldeggiata la formula scritta: in sede di ispezione il Titolare potrà facilmente mostrarla.

Un altro aspetto importante su cui insistono le Linee Guida è il **diritto alla revoca online** da parte dell'Interessato.

Tuttavia, quando il consenso viene prestato per via elettronica con un solo clic di mouse, un solo scorrimento o premendo un tasto, l'Interessato deve, in pratica, poterlo revocare con altrettanta facilità. Se il consenso è espresso attraverso un'interfaccia utente specifica di servizio (ad esempio un sito web, un'applicazione, un account protetto, l'interfaccia di un dispositivo IoT oppure posta elettronica), è indubbio che l'Interessato deve poterlo revocare tramite la medesima interfaccia elettronica.

Anche la modalità del diritto di revoca non va sottostimata: nel documento si legge l'esempio di un comportamento a rischio sanzione. Se per un festival di musica si chiede il consenso per finalità di marketing online, mentre la revoca deve essere comunicata a un ufficio in certi orari settimanali e lavorativi, la revoca non è a norma perché il consenso dovrebbe essere revocabile rapidamente online 24 ore su 24. Ovviamente il Titolare deve aver predisposto i meccanismi per sospendere il trattamento dei dati personali di un Interessato nel caso quello revochi il consenso.

Altri capitoli sono dedicati al **consenso dei minori**, argomento assai spinoso sul quale la Commissione Europea ha allo studio un progetto di legge basato su uno Spid europeo attivabile solo dai genitori in caso di minori di 14 anni per l'Italia, 16 per gli altri Paesi. Richiamandosi a quanto