Cristina Vicarelli

Avvocato

GDPR e sicurezza informatica: è vero che sono in antitesi?

e-privacy 2018 - summer edition

- «dato personale»: qualsiasi informazione **riguardante** una **persona fisica** identificata o **identificabile** («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o **indirettamente**, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

(GDPR art. 4)

Esempio di dati personali:

- nome e cognome;
- indirizzo di casa;
- indirizzo e-mail, come nome.cognome@azienda.com;
- numero della carta d'identità;
- dati sulla posizione (ad es. la funzione di posizionamento su un telefono cellulare)*;
- un indirizzo IP (Internet Protocol);
- un ID cookie*;
- l'identificativo pubblicitario del proprio telefono;
- i dati conservati in un ospedale o da un medico, che possono essere un simbolo che identifica univocamente una persona.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_it (di saguito indicato anche come TOOL COM UE)

Cristina Vicarelli
Avvocato

- Per quanto concerne le persone identificate o identificabili "indirettamente", questa categoria rimanda tipicamente al fenomeno delle "combinazioni uniche", siano esse ampie o ridotte. Nei casi in cui, a prima vista, gli identificatori disponibili non consentono di identificare una persona particolare, si può ancora considerare quella persona "identificabile" **perché quelle informazioni combinate con altre (che siano o meno conservate dal *titolare* del trattamento) consentiranno di distinguerla dalle altre.**

(WP29 - Parere 4/2007 sul concetto di dati personali - WP 136)

- i fornitori di accesso Internet e i gestori delle reti LAN possono, utilizzando mezzi ragionevoli, identificare gli utenti Internet cui essi hanno attribuito indirizzi IP, poiché, normalmente, essi “registrano” in un apposito file la data, l'ora, la durata e l'indirizzo IP dinamico assegnato all'utente Internet. Lo stesso dicasi per i fornitori di servizi Internet, i quali detengono un registro sul server HTTP In questi casi, non vi è dubbio sul fatto che si possa parlare di dati personali (on-line, adottato il 21.11.2000.

- (WP 37: Tutela della vita private su Internet – Un approccio integrato dell'UE alla protezione dei dati)

- In particolare, nei casi in cui il trattamento di indirizzi IP viene effettuato per identificare gli utenti di un computer (ad esempio, dal titolare di un diritto d'autore per perseguire l'utente di un computer per violazione di diritti di proprietà intellettuale), il responsabile del trattamento parte dal principio che **i "mezzi che possono essere ragionevolmente utilizzati" per identificare le persone esistono, ad esempio nella figura del giudice del ricorso** (altrimenti la raccolta delle informazioni non avrebbe senso), e quindi tali informazioni andrebbero considerate dati personali.

(WP29 - Parere 4/2007 sul concetto di dati personali - WP 136)

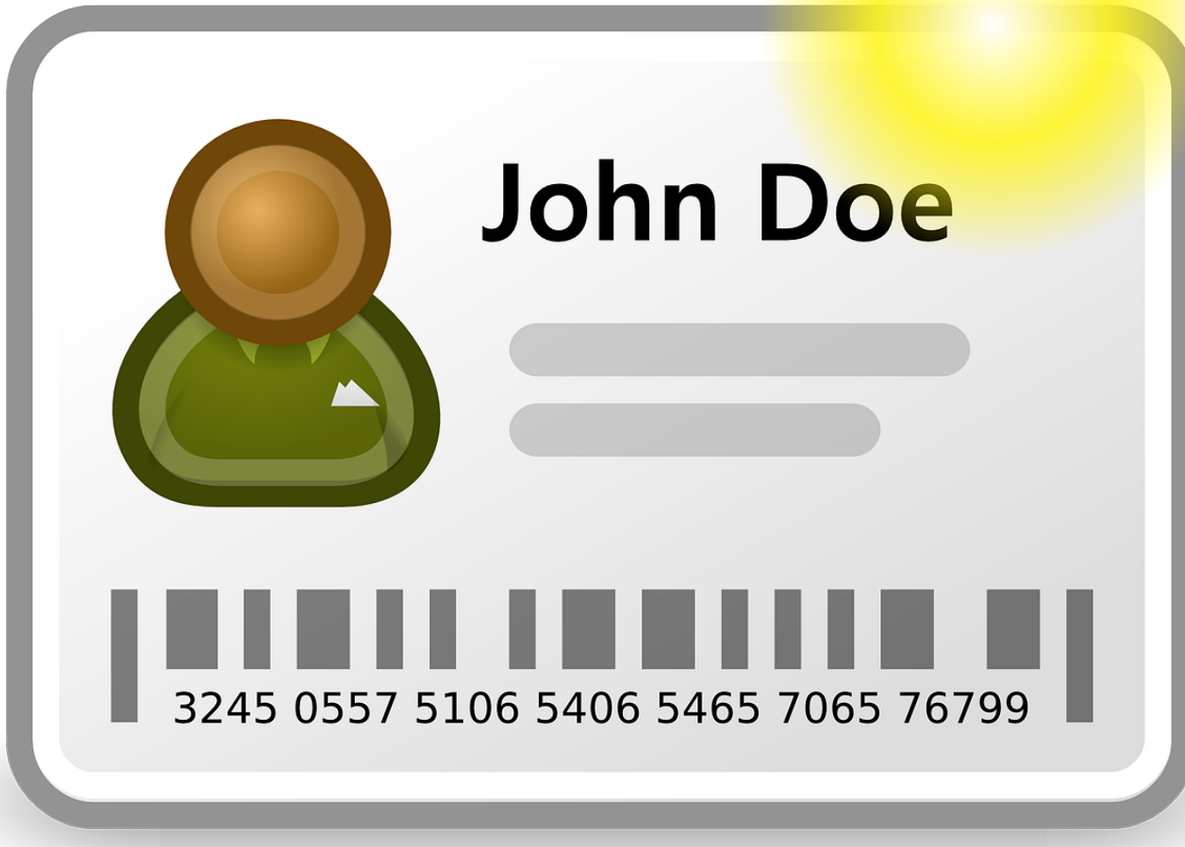
Un caso particolare è quello di alcuni tipi di **indirizzi IP che, in alcune circostanze, non permettono effettivamente di identificare l'utente** per vari motivi tecnici ed organizzativi. Si pensi per esempio agli indirizzi IP attribuiti a un computer di un **internet café,** dove non è richiesta l'identificazione dei clienti. Si potrebbe affermare che i dati raccolti sull'impiego del computer X per un certo lasso di tempo non consentono di identificare l'utente con mezzi ragionevoli, e quindi non si può parlare di dati personali. Tuttavia, occorre notare che **i fornitori di servizi Internet molto probabilmente non sapranno se gli indirizzi IP in questione permettono l'identificazione o meno, e tratteranno i dati associati con quell'IP nello stesso modo in cui trattano le informazioni associate agli indirizzi IP degli utenti debitamente registrati e identificabili.**

Pertanto, **a meno di poter distinguere con assoluta certezza che i dati corrispondano a utenti non identificabili, il fornitore di servizi Internet dovrà trattare tutte le informazioni IP come dati personali, per maggiore sicurezza.**

(WP29 - Parere 4/2007 sul concetto di dati personali - WP 136)

Cristina Vicarelli
Avvocato

I dati personali sottoposti a deidentificazione, cifratura o pseudonimizzazione, ma che possono essere utilizzati per reidentificare una persona, rimangono dati personali e rientrano nell'ambito di applicazione della normativa.



Cristina Vicarelli
Avvocato

Corte di Giustizia

- Sentenza C-582/14 (sentenza 19 ottobre 2016 “Breyer”)

- 1. (…) un indirizzo di protocollo Internet dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un **dato personale** (…) qualora detto fornitore disponga di **mezzi giuridici** che gli consentano di **far identificare** la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone.

Cristina Vicarelli
Avvocato

2. L’articolo 7, lettera f), della direttiva 95/46 dev’essere interpretato nel senso che **osta** a una normativa di uno Stato membro ai sensi della quale un fornitore di servizi di media online può raccogliere e impiegare dati personali di un utente di tali servizi, **in mancanza del suo consenso**, solo nella misura in cui detta raccolta e detto impiego siano necessari per **consentire e fatturare l’effettiva fruizione dei suddetti servizi** da parte dell’utente in questione, senza che l’obiettivo di assicurare il funzionamento generale dei medesimi servizi possa giustificare l’impiego di tali dati dopo una sessione di consultazione degli stessi.

Cristina Vicarelli
Avvocato

legittimo interesse del titolare

- “Infatti, mentre l’articolo 7, lettera f), si riferisce, in maniera generale, al «perseguimento dell’interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati», l’articolo 15 del TMG autorizzerebbe il fornitore di servizi a raccogliere e impiegare dati personali di un utente solamente nella misura in cui ciò sia necessario per consentire e fatturare l’effettiva fruizione dei media online. L’articolo 15 della TMG osterebbe quindi, in maniera generale, alla conservazione, al termine di una sessione di consultazione di media online, di dati personali per garantire la fruizione di tali media. Orbene, **i servizi federali tedeschi che forniscono servizi di media online potrebbero altresì avere un interesse legittimo a garantire, al di là di ciascuna effettiva fruizione dei loro siti Internet accessibili al pubblico, la continuità del funzionamento di detti siti.**

- 61 Come rilevato dall’avvocato generale ai paragrafi 100 e 101 delle sue conclusioni, una normativa nazionale siffatta non si limita a precisare, conformemente all’articolo 5 della direttiva 95/46, la nozione di «interesse legittimo» di cui all’articolo 7, lettera f), di tale direttiva.

- 62 A tale riguardo, occorre altresì ricordare che **l’articolo 7, lettera f), della suddetta direttiva osta a che uno Stato membro escluda in modo categorico e generalizzato la possibilità che talune categorie di dati personali siano oggetto di trattamento, senza consentire la ponderazione dei diritti e degli interessi contrapposti in gioco nel caso specifico.** Uno Stato membro non può quindi stabilire per tali categorie, in modo definitivo, il risultato della ponderazione dei diritti e degli interessi contrapposti, **senza consentire un diverso risultato in ragione delle circostanze specifiche del caso concreto** (v., in tal senso, sentenza del 24 novembre 2011, ASNEF e FECEMD, C-468/10 e C-469/10, EU:C:2011:777, punti 47 e 48).

- 63 Orbene, una normativa come quella di cui al procedimento principale riduce, con riferimento al trattamento di dati personali degli utenti di siti di media online, la portata del principio previsto all’articolo 7, lettera f), della direttiva 95/46, escludendo che **l’obiettivo di garantire il funzionamento generale di tale medium online possa essere oggetto di ponderazione con l’interesse o i diritti e le libertà fondamentali di detti utenti, diritti e libertà che richiedono, conformemente alla disposizione in parola, tutela** ai sensi dell’articolo 1, paragrafo 1, di tale direttiva.”

Cristina Vicarelli
Avvocato

GDPR considerando 49

- Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in **misura strettamente necessaria e proporzionata** per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di **resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi** che compromettano la **disponibilità,** l'**autenticità**, l'**integrità** e la **riservatezza** dei dati personali conservati o trasmessi e la **sicurezza dei relativi servizi** offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), **fornitori** di reti e servizi di comunicazione elettronica e **fornitori** di tecnologie e servizi di sicurezza. **Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica**.

Cristina Vicarelli
Avvocato

come funziona il legittimo interesse?

- 1. individuazione della base giuridica: articolo 6 GDPR liceità del trattamento comma 1 lettera f): “il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore”.

Cristina Vicarelli
Avvocato

- 3) individuare il legittimo interesse del titolare o di un terzo

- 4) dimostrare che il trattamento dei dati personali (che deve essere corretto, pertinente e non eccedente) è necessario a perseguire il legittimo interesse individuato

- 5) operare il **bilanciamento degli interessi** vero e proprio, giustificando perché il legittimo interesse prevale su interessi libertà e diritti dell'interessato.

- Se non è possibile dimostrare i punti 4 e 5 il legittimo interesse non si può utilizzare come base giuridica e il trattamento relativo non si può operare.

Cristina Vicarelli
Avvocato

Accountability

- Il **bilanciamento degli interessi** posto alla base del trattamento va **documentato per iscritto** (art. 5 comma 2 del GDPR: il Titolare deve essere in grado di comprovare il rispetto dei principi che presiedono al trattamento)

- “documentare questa valutazione. Così com’è adattabile il livello di dettaglio con cui deve essere svolta la valutazione, deve essere adattabile anche l’entità della documentazione. Detto ciò, deve essere disponibile una documentazione di base in tutti i casi **fuorché nei più insignificanti,** a prescindere dalla valutazione dell’impatto del trattamento sulla persona. È sulla base di tale documentazione che la valutazione del *titolare* del trattamento potrà essere ulteriormente esaminata ed eventualmente contestata” WP 217;

Cristina Vicarelli
Avvocato

Infine: occorre dichiarare nell'**informativa** il legittimo interesse usato come base giuridica (cfr. artt. 13 e 14 del GDPR)

Cristina Vicarelli
Avvocato

L’interessato può opporsi al trattamento?

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'**articolo 6, paragrafo 1**, lettere e) o **f)**, compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali **salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato** oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. (Art. 21 GDPR)

Avv. Cristina Vicarelli

studiolegale@cristinavicarelli.it
Twitter @cristi_vic
www.cristina-vicarelli.it