PUNTO DIGITALE FACILE

# Il difficile rapporto tra privacy e web

# Che cos'è la privacy?

PUNTO DIGITALE FACILE

Con il termine "**privacy**" si fa riferimento al diritto a proteggere la propria sfera privata.

# La privacy e i diritti umani

Il **diritto alla privacy** e alla protezione dei dati personali costituisce un diritto fondamentale delle persone.

Collegato direttamente alla tutela della dignità umana, come sancito dalla carta dei diritti fondamentali dell'Unione Europea

# Le tracce in rete...

- Informazioni in rete o **dati**.
- **Registrate** e **studiate**.

Quando navighiamo in internet, lasciamo inevitabilmente delle tracce, dei dati. Queste informazioni vengono registrate e analizzate dalle varie aziende, titolari dei vari siti o social che visitiamo e vengono rielaborate, al solo fine di creare pubblicità personalizzata e mirata.

# Dati raccolti da Google

- ❑ **Attività**
- ❑ **Creazioni**
- ❑ **Dati personali**

Attività: Informazioni di ricerche fatte su siti o social network inerenti ad annunci o video visti e posizione personale con indirizzo IP

Creazioni: Dati estratti dall'account durante l'invio o ricezione mail utilizzo dei contatti o creazione di eventi sul calendario o condivisione di elementi su cloud (Es. Drive)

Dati personali: Informazioni di base Che si indicano durante la registrazione In una piattaforma (Es. nome, indirizzo Mail, numero di telefono, sesso, PSW, data di nascita e paese di provenienza)

# Dati raccolti da FaceBook

- Dati personali
- Interazioni

INTERAZIONI: sono le azioni che effettuiamo sui social (Es. post, like, condivisioni, immagini) registrate ed analizzate per la profilazione di pubblicità personalizzata

# Dati raccolti da Amazon

PUNTO DIGITALE FACILE

- Dati di **navigazione**.
- Tracce degli ordini.
- Tracce degli acquisti.

# Profilazione

PUNTO DIGITALE FACILE

È il processo di ricostruzione delle informazioni personali.

# Pro e contro

Un social network è una **"piazza virtuale"** in cui si possono scambiare idee e opinioni di ogni genere.
Il **Comitato economico e sociale europeo** sul tema "l'impatto sui siti di social network", elenca una serie di pro e contro collegati all'uso dei social network.

**Pro:**

- garantire ed esercitare la libertà di espressione;
- creare gruppi on-line e consentire la loro aggregazione;
- fare nuove amicizie, ritrovare amici e parenti e poter comunicare con loro;
- prevenire situazioni rischiose con richieste di aiuto;
- promuovere beni e servizi incrementando in tal modo il commercio elettronico;
- condividere informazione che riguardano la salute.

**Contro:**

- possibili traumi psicologici causati da insulti trasmessi attraverso tali siti;
- molestie sessuali;
- annunci espliciti di prostituzione;
- ripetuta violazione della privacy, dell'onore e della dignità personale;
- incitamento alla violenza e razzismo;
- diffusione di ideologie perseguibili dalla legge.

PUNTO DIGITALE FACILE

# Social network e reati

# Fonti normative:

In via prevalente, la **privacy** è disciplinata da:

- Carta dei diritti fondamentali dell'Unione Europea;
- General Data Protection Regulation (GDPR);
- Codice in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003 n. 196, così come novellato dal D.lgs. 101/2018)
- Linee Guida/Provvedimenti del Garante per la privacy;
- Autorizzazioni Generali del Garante per la privacy.

→ **Tutti gli stati firmatari hanno dovuto emanare dei decreti interni che recepissero quanto sancito dal Regolamento Europeo 2016/679.**
**In Italia è stato emanato il Decreto Legislativo 101/2018 che ha modificato la parte generale del Codice Privacy allora vigeva.**

# Il Garante per la privacy

- ❑ **Autorità amministrativa indipendente**
- ❑ **Organo collegiale**
- ❑ **Resta in carica per 7 anni**

I principali **compiti** del Garante sono:

- controllo sul rispetto della disciplina privacy;
- risoluzione di casi specifici;
- emanazione di atti;
- educazione alla privacy;
- irrogazione di sanzioni amministrative;
- consulenza al Parlamento e Governo;
- relazione al Parlamento e Governo.

PUNTO DIGITALE FACILE

Le **principali sanzioni** in ambito di **tutela dei dati personali**, così come individuate dal nostro codice della Privacy (d.lgs. 196/2003).

## SANZIONI

| CONDOTTA | SANZIONE AMMINISTRATIVA | SANZIONE PENALE | ENTITA'* (in blu le sanzioni amministrative in rosso le sanzioni penali) |
|---|---|---|---|
| Omessa o inidonea informativa | ✅ | ⚠️ | art. 161: da 2.400 € a 2.400.00 €<br>art. 167: da 6 mesi a 3 anni di reclusione |
| Cessione non autorizzata di dati personali | ✅ | ⚠️ | art. 162, 1 comma: da 4.000 € a 2.400.000 €<br>art. 167: da 6 mesi a 3 anni di reclusione |
| Mancata adozione delle misure minime di sicurezza | ✅ | ✅ | art. 162, comma 2bis: da 10.000 € a 2.400.000 €<br>art. 169: arresto fino a 2 anni (possibile oblazione entro 6 mesi) |
| Violazione del diritto di opposizione ("Registro delle opposizioni") | ✅ | ⚠️ | art. 162, comma 2quater: da 10.000 € a 2.400.000 €<br>art. 167: da 6 mesi a 3 anni di reclusione |
| Conservazione dei dati di traffico telefonico o telematico oltre i limiti consentiti | ⚠️ | ⚠️ | art. 162bis: da 10.000 a 50.000 euro (salvo che il fatto non costituisca reato) |
| Mancata "Data Breach Notification" (violazione dati personali subita da un fornitore di servizi di comunicazione elettronica) | ✅ | 🚫 | art 162ter, comma 1: da 10.000 € a 2.400.000 €<br>art. 162ter, comma 2-3: da 60 euro al 5% del fatturato nell'ultimo esercizio. |
| Inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto del Garante | ✅ | 🚫 | art. 162, comma 2ter: da 12.000 € a 2.400.000 € |
| Omessa o incompleta notificazione al Garante | ✅ | 🚫 | art. 163: da 8.000 € a 2.400.000 € |
| Omessa informazione o esibizione al Garante | ✅ | 🚫 | art. 164: da 4.000 € a 2.400.000 € |
| Trattamento illecito di dati | ✅ | ✅ | art. 162, comma 2bis: da 10.000 € a 2.400.000 €<br>art. 167: reclusione da 6 mei a 3 anni |
| Falsità nelle dichiarazioni e notificazioni al Garante | 🚫 | ✅ | art. 168: reclusione da 6 mesi a 3 anni |
| Inosservanza dei provvedimenti del Garante | 🚫 | ✅ | art. 170: reclusione da 3 mesi a 2 anni |

* l'entità degli importi delle sanzioni amministrative tengono conto dei *"casi di minore gravità e ipotesi aggravate"* di cui all'art. 164bis del d.lgs. 196/03

LEGENDA ✅ SI ⚠️ dipende 🚫 NO

# La diffamazione è reato!

PUNTO DIGITALE FACILE

- **Diffamazione**
- Reato **punito dall'art. 595 del Codice Penale**
- È reato tale quando la **persona offesa non è presente**

# Ingiuria vs Diffamazione

## Ingiuria

offesa proferita direttamente al destinatario della stessa, quindi in sua presenza

**non è più reato** (resta solo l'illecito civile che dà diritto al risarcimento del danno cui il giudice aggiunge il pagamento di una multa)

## Diffamazione

offesa rivolta a qualcuno, detta in sua assenza davanti a più di una persona (quindi, se riferita a una sola persona, a titolo di sfogo o confidenza, non è reato).

**resta un illecito penale**

PUNTO DIGITALE FACILE

# Diffamazione aggravata

PUNTO DIGITALE FACILE

"La diffusione di un messaggio diffamatorio attraverso l'uso di qualsiasi social network integra un'ipotesi di **diffamazione aggravata** ai sensi dell'art. 595 del Codice Penale, poiché trattasi di **condotta potenzialmente capace di raggiungere un numero indeterminato o comunque quantitativamente apprezzabile di persone**".

# Il reato di diffamazione

Art. 595 del Codice Penale

PUNTO DIGITALE FACILE

## In che cosa consiste?

Nell'offendere l'altrui reputazione comunicando con più persone

## Come è punibile?

Solo a querela, che deve essere presentata entro 90 giorni da quando la persona offesa ha avuto notizia del fatto

## Le pene

| | Carcere | Multa |
|---|---|---|
| Diffamazione semplice | fino a **1 anno** | fino a **1.032 euro** |
| Diffamazione con attribuzione di un fatto determinato | fino a **2 anni** | fino a **2.065 euro** |
| Diffamazione a mezzo stampa | da **6 mesi** a **3 anni** | più di **516 euro** |

Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza, o ad una Autorità costituita in collegio, le pene sono aumentate

ANSA-CENTIMETRI

# Furto d'identità

- **Furto di identità**
- Reato penale


PUNTO DIGITALE FACILE

- Modificare le password di tutti gli account online.
- Se il furto di identità si realizza tramite un sito web o social network, contattare il relativo servizio di sicurezza o di assistenza per disconoscere l'account e per chiederne il blocco.
- In caso di sottrazione e pubblicazione di foto o video inoltrare una formale richiesta di cancellazione al sito in questione.
- In caso non si riuscisse a ottenere la cancellazione, rivolgersi al Garante della protezione dei dati personali mediante ricorso o, per casi più gravi/urgenti, contattare la Polizia Postale.
- In caso di furto di identità, di profili social o dell'account di posta elettronica fare subito una denuncia a un ufficio di Polizia/Polizia Postale per accesso telematico abusivo e sostituzione di persona.

# “Intrusioni” nei profili social

**Entrare senza permesso nei profili social del partner è un vero e proprio reato.**

La Polizia Postale ha rilevato un aumento considerevole di querele sporte da mogli e mariti che si ritrovano spiati su Facebook dal partner (o dall’ex dal quale si sono separati): l’art. 615-ter del Codice Penale, punisce espressamente un tale comportamento, insieme agli accessi abusivi in sistemi informatici o telematici.

# Social e rischi nel lavoro

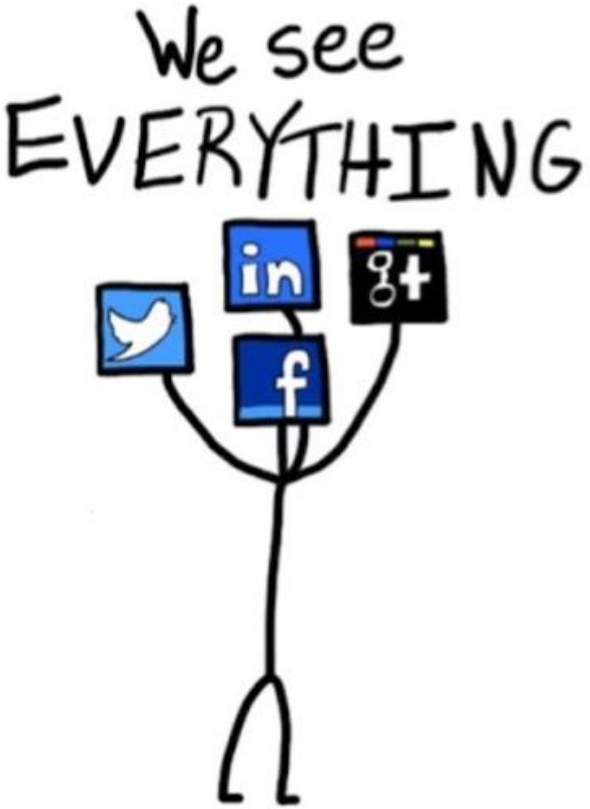
## Facebook può davvero farti licenziare

PUNTO DIGITALE FACILE

Diverse sentenze hanno sancito il principio della legittimità del licenziamento del lavoratore che fa un uso improprio dei social network pubblicando post (o anche solo mettendo like o condividendo) contenenti giudizi, affermazioni, offese riconducibili al datore di lavoro o all'azienda in cui in cui lavora.

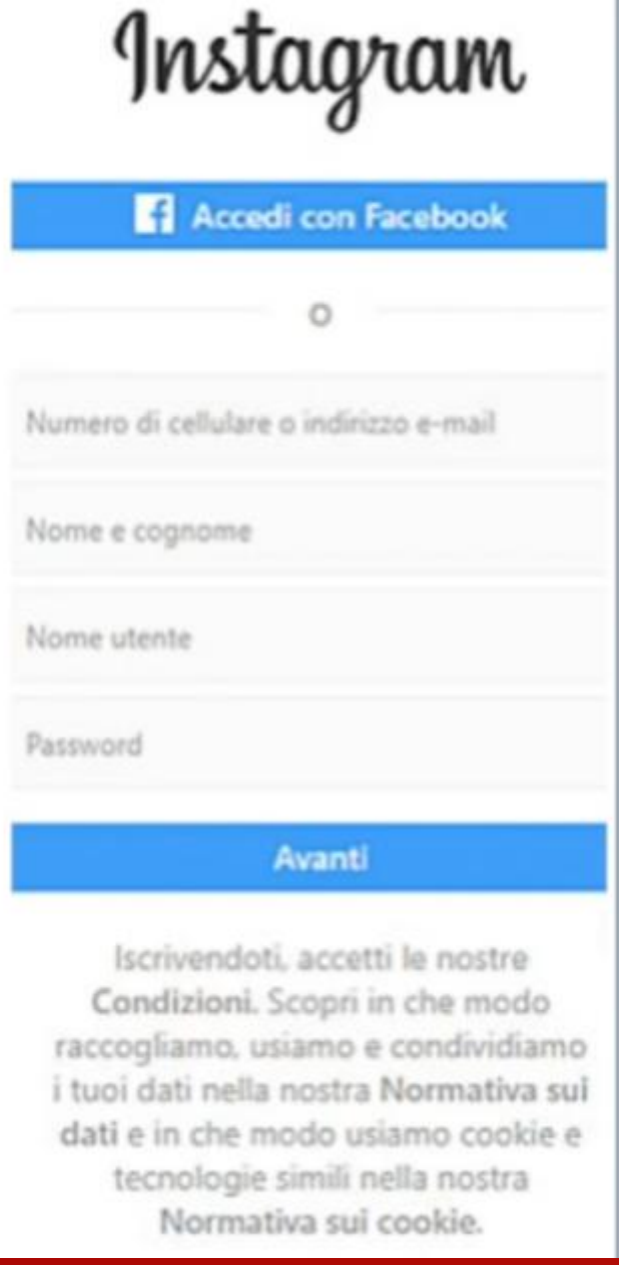
PUNTO DIGITALE FACILE

# Privacy nei vari Social Network



# Creare un account social

Quando ci si iscrive su un Social Network si acconsente al **trattamento dei dati personali**: l'utente sottoscrive un contratto di **licenza d'uso** con il quale **cede al social network tutto quello che viene pubblicato a suo nome**.




# Il consenso digitale del minore

- Il decreto del GDPR in Italia fissa a **14 anni** l'età minima per l'espressione del consenso al trattamento dei propri dati personali.
- L'Art. 8 del GDPR europeo fissa a **16 anni** l'età per l'offerta diretta di servizi della società dell'informazione ai minori.
- Il GDPR europeo fissa quella soglia minima per servizi quali i social network o i servizi di messaggistica, per "***tutelare il minore in quei contesti virtuali ove risulta maggiormente esposto a causa di una minore consapevolezza dei rischi insiti nella rete***".

# FaceBook e Messanger

PUNTO DIGITALE FACILE

- Con l'adeguamento al GDPR, i giovani **tra i 13 e i 15 anni** hanno bisogno del consenso di un genitore per usare il social.
- Senza il **consenso dei genitori**, i ragazzi vedranno una versione meno personalizzata della piattaforma, con condivisione limitata e annunci meno rilevanti.
- Il sistema di controllo prevede che chi ha un'età inferiore ai 16 indichi il **contatto sul social** o l'**indirizzo email** del genitore che darà il consenso.

# WhatsApp

PUNTO DIGITALE FACILE

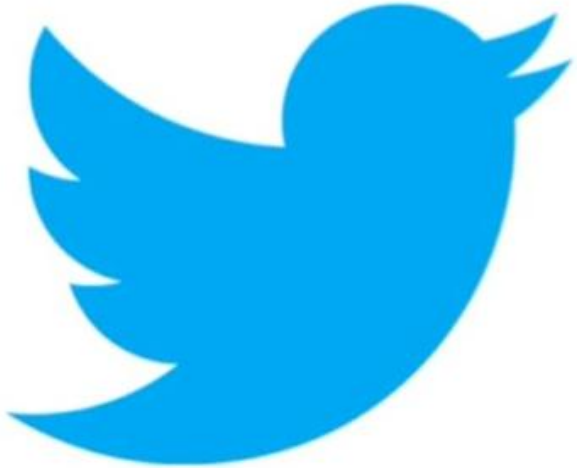
- Anche la chat più usata richiede un'autorizzazione ai genitori dei ragazzi **tra i 13 e i 15 anni**, ma solo nell'Unione Europea.
- Senza il consenso dei genitori, tutti i ragazzi di età inferiore ai 16 non potranno usare la chat.

**WhatsApp**

# Twitter

PUNTO DIGITALE FACILE

- Il microblog ha innalzato da 13 a **16 anni** l'età minima richiesta agli europei per usare Periscope.
- L'app, acquistata da Twitter nel 2015, serve per fare dirette video con lo smartphone.



# Instagram

PUNTO DIGITALE FACILE

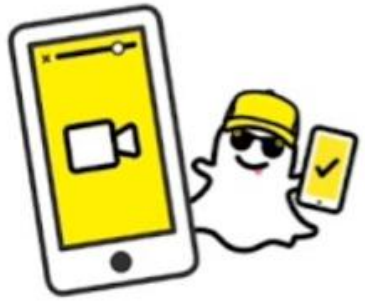
- Il social delle immagini permette all'utente di richiedere una copia di tutto quanto ha condiviso sulla piattaforma (foto, video, messaggi).
- Il limite d'età non è stato aggiornato, al momento resta fermo a **13 anni**.

Instagram

# Snapchat

PUNTO DIGITALE FACILE

- La chat di messaggi che scompaiono richiede per registrarsi una mail o un numero di cellulare.
- L'età non viene chiesta, ma nelle condizioni d'uso, si scopre che "*i servizi* ***non si rivolgono a persone sotto i 13 anni****. Questo spiega perché non raccogliamo consapevolmente dati personali di soggetti con un'età inferiore ai 13 anni*".
- Nel 2013, Snapchat ha creato SnapKids, una versione ridotta dell'app per chi ha tra 8 e 12 anni.



# Telegram

PUNTO DIGITALE FACILE

- La chat, apprezzata per la riservatezza, in fase di registrazione chiede solo il **numero di telefono**.
- Non sono stati fatti annunci di conformità al GDPR.

# Pubblicazione delle foto online

PUNTO DIGITALE FACILE

- La pubblicazione di una fotografia online rientra nel tema del trattamento di dati personali ed è da considerarsi interferenza nella vita privata.
- Bisogna prestare particolare attenzione nel pubblicare immagini di minori.
- In una sentenza del **tribunale di Mantova** (novembre 2017) il giudice ha stabilito che per la pubblicazione delle foto dei figli **occorre il consenso di entrambi i genitori**. Senza il consenso dei due genitori, la foto non è pubblicabile.

PUNTO DIGITALE FACILE

# Dati personali e curriculum vitae

# Curriculum vitae e trattamento dati personali

PUNTO DIGITALE FACILE

- Quando si cerca lavoro è normale preparare un proprio curriculum vitae.
- Nel del CV sono riportati **dati sulla nostra persona**, utili da far conoscere a chi potrebbe essere interessato a selezionarci per un lavoro e per contattarci rispetto a future ricerche di lavoro.
- Anche l'operazione di contatto consiste in un trattamento di dati che va autorizzato con l'inserimento di una **specifica autorizzazione** al trattamento e facendo riferimento alle normative in materia (l'art. 13 del d.lgs.196/2003 e l'art. 13 GDPR 679/16).
- Si può **circoscrivere** l'autorizzazione alle sole finalità connesse alla selezione del personale.
- Prima del Decreto Legislativo 101/2018, l'inserimento nel CV dell'autorizzazione al trattamento dei dati era considerata obbligatoria. In seguito, è diventata un'opportunità che ognuno può decidere se riportare o meno.
- Può essere utile autorizzare il datore di lavoro, tramite il curriculum, al trattamento dei dati così che questi possa utilizzarli fin da subito per un contatto.
- L'autorizzazione al trattamento **va inserita al fondo della pagina** e comunque prima della necessaria firma da apporre sul CV.

# Alcuni esempi di situazioni che ci sembrano normali ma che in realtà violano la privacy

PUNTO DIGITALE FACILE

1. Invio di email con destinatari visibili

Un’azienda invia una newsletter a tutti i clienti usando il campo "A" o "CC" invece di "CCN", rivelando gli indirizzi email di tutti i destinatari.

2. Condivisione errata di documenti con dati sensibili

Un ufficio invia un documento Excel contenente dati di clienti (nomi, numeri di telefono, email, codici fiscali) a più destinatari senza crittografarlo o senza verificare che i destinatari siano autorizzati a riceverlo.

3. Foto di gruppo pubblicate sui social senza consenso

Un’organizzazione scatta una foto di gruppo durante un evento e la pubblica online senza chiedere il consenso ai partecipanti riconoscibili nella foto.

4. Discussione di dati sensibili in un'email inoltrata

Un medico invia via email informazioni cliniche a un paziente, ma poi inoltra la stessa email a un altro paziente per errore, rivelando informazioni sanitarie non destinate a lui.

5. Messaggi WhatsApp o chat aziendali con informazioni private

Un responsabile di un'azienda condivide in una chat WhatsApp informazioni riservate sui dipendenti, come assenze per malattia o dettagli sulle retribuzioni.

6. Stampa e distribuzione errata di documenti

In un ufficio, un dipendente stampa un documento con dati personali riservati, ma lo dimentica sulla stampante accessibile a tutti.

7. Condivisione di informazioni sanitarie via email non protetta

Un ospedale invia un'email ai pazienti per comunicare esiti di analisi mediche, ma non usa alcuna misura di protezione (es. email crittografata o sistema protetto).

8. Registrazione di una telefonata senza consenso

Un'azienda registra una conversazione telefonica con un cliente senza informarlo prima, violando il diritto alla privacy.

9. Dati personali lasciati visibili in un database pubblico

Un'azienda pubblica online un elenco di clienti o fornitori con nomi, indirizzi e numeri di telefono senza restrizioni di accesso.

10. Moduli di iscrizione a eventi visibili a tutti

Un'organizzazione raccoglie adesioni per un evento con un foglio cartaceo esposto pubblicamente, dove chiunque può vedere i nomi e le email degli altri iscritti.

**In tutti questi casi, la violazione avviene perché i dati personali vengono diffusi involontariamente o senza misure di protezione adeguate. Il GDPR prevede che chi raccoglie e tratta dati personali debba adottare misure di sicurezza adeguate per prevenire divulgazioni non autorizzate.**

# Alcuni sanzioni per violazioni della privacy inflitte dal Garante per la protezione dei dati personali in Italia

1. OpenAI (ChatGPT) – €15 milioni

- Nel dicembre 2024, il Garante ha multato OpenAI, sviluppatore di ChatGPT, per aver trattato i dati personali degli utenti senza una base legale adeguata e per violazioni dei principi di trasparenza e obblighi informativi.

2. Meta Platforms Inc. – €1 milione

- Nel gennaio 2023, il Garante ha sanzionato Meta per violazioni relative al trasferimento di dati personali verso paesi terzi senza le necessarie garanzie previste dalla legge. PrivacyStudio

3. Wind Tre S.p.A. – €16,7 milioni

- Nel luglio 2020, il Garante ha multato Wind Tre per pratiche di telemarketing aggressive e per aver trattato i dati personali degli utenti senza un valido consenso.

4. Eni Gas e Luce – €11,5 milioni

- Nel gennaio 2020, Eni Gas e Luce è stata sanzionata per attività di telemarketing indesiderato e per l'attivazione di contratti non richiesti, violando le normative sulla protezione dei dati personali.

5. TIM S.p.A. – €27,8 milioni Il Sole 24 ORE

- Nel gennaio 2020, il Garante ha imposto una multa a TIM per aver effettuato attività promozionali senza il consenso degli interessati e per la gestione inadeguata delle liste di opposizione.

6. Facebook Ireland Ltd. – €1 milione Reuters Wikipedia, l'enciclopedia libera+9ecommercelegale.it+9

- Nel novembre 2018, Facebook è stata multata per il caso Cambridge Analytica, in cui i dati personali degli utenti italiani sono stati trattati in modo illecito.

7. Fastweb S.p.A. – €4,5 milioni

- Nel luglio 2016, Fastweb è stata sanzionata per aver effettuato attività di telemarketing senza il consenso degli interessati e per l'assenza di misure di sicurezza adeguate nella gestione dei dati personali.

8. Vodafone Italia S.p.A. – €12,25 milioni Wikipedia, l'enciclopedia libera

- Nel novembre 2020, Vodafone è stata multata per attività di telemarketing illecito e per il trattamento non autorizzato dei dati personali degli utenti.

9. Sky Italia S.r.l. – €3,2 milioni

- Nel dicembre 2019, Sky Italia è stata sanzionata per aver effettuato attività promozionali senza il consenso degli interessati e per la gestione inadeguata delle liste di opposizione.

10. Iren Mercato S.p.A. – €3 milioni Garante Privacy e Wikipedia

- Mercato aveva ottenuto liste di anagrafiche da una società terza, che a sua volta le aveva acquisite da altre due aziende. Sebbene i clienti avessero inizialmente fornito il consenso per attività promozionali da parte di terzi, tale consenso non copriva le successive cessioni dei dati a ulteriori titolari. Questo ha portato a contatti promozionali senza un consenso specifico e informato degli interessati.

# Consigli pratici per tutelare la tua privacy, sia online che nella vita quotidiana

PUNTO DIGITALE FACILE

1. Usa password sicure e diverse per ogni servizio.

Evita nomi, date di nascita o “123456”. Meglio usare un gestore di password.

2. Attiva sempre l’autenticazione a due fattori (2FA).

Soprattutto per email, banca, social e servizi cloud.

3. Controlla i permessi delle app.

Disattiva accessi inutili a fotocamera, microfono, posizione o contatti.

4. Naviga con attenzione.

Usa browser sicuri, modalità incognita quando serve, e stai lontano da siti non https.

5. Fai attenzione ai social.

Rivedi le impostazioni sulla privacy e condividi meno dati possibili con sconosciuti.

PUNTO DIGITALE FACILE

6. Diffida di link sospetti.

Email, SMS o messaggi WhatsApp strani? Non cliccare, potrebbe essere phishing.

7. Blocca numeri spam.

Su Android e iPhone puoi bloccare numeri manualmente o usare app come Truecaller o Dov'è il mio telefono per filtrare chiamate truffa.

8. Eliminati dalle newsletter indesiderate.

Cerca in fondo all'email il link "unsubscribe" o "annulla iscrizione". Se non funziona, segnalala come spam.

9. Pulisci i tuoi account.

Chiudi quelli che non usi più e chiedi la cancellazione dei dati. È un tuo diritto (art. 17 GDPR).

10. Proteggi anche chi ti sta vicino.

Non condividere mai numeri, email o foto di altri senza il loro consenso.

# Sitografia

- **Garante per la privacy** - https://bit.ly/2HfaWqf
- **Privacy e sicurezza informatica** - https://bit.ly/2JwarJY
- **Facebook, il post offensivo è diffamazione aggravata** - https://bit.ly/2LAnqNz
- **Generazioni Connesse** - https://bit.ly/2vRSqhd
- **Commissariato di Polizia Postale online** - https://bit.ly/2JyzkF3
- **Data Selfie svela i dati raccolti da Facebook** - https://bit.ly/2VxQR7A

PUNTO DIGITALE FACILE

# GRAZIE PER L'ATTENZIONE