

WEBINAR

**Privacy e Acquisti Online: diritti
tutele e responsabilità per imprese e consumatori**

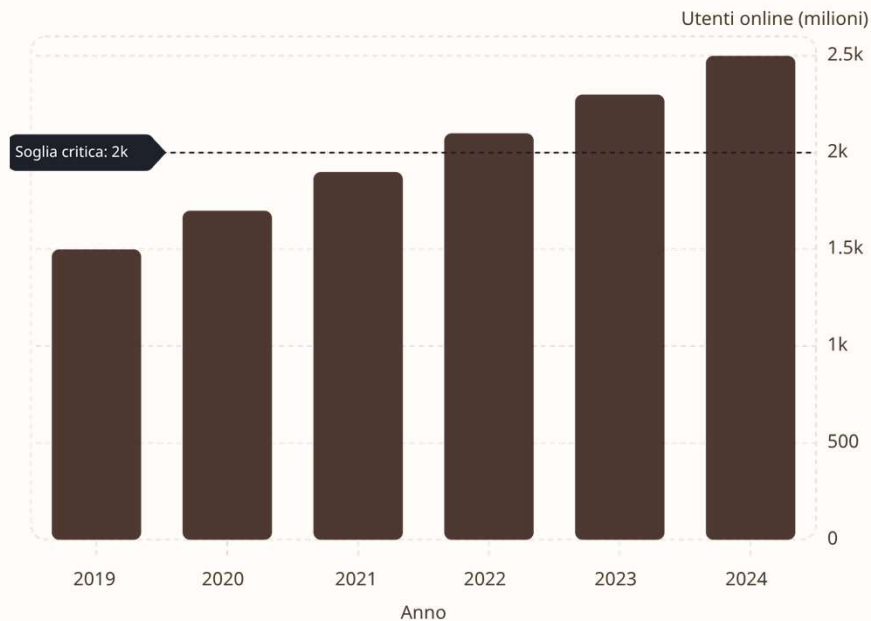
*in collaborazione con
Laboratorio Chimico Camera di Commercio Torino
e U.Di.Con. Piemonte*

Torino, 15.07.2026

Diritti, Tutele e Responsabilità nell'Era Digitale

La Rivoluzione Digitale: Il Nuovo Marketplace

La materia degli acquisti online è organizzata sostanzialmente da due disposizioni fondamentali: il Regolamento (UE) 2016/679 (GDPR) in tema di protezione dei dati personali, e la disciplina consumeristica contenuta nel D.Lgs. n. 206/2005 (Codice del Consumo). A questi si affianca il Regolamento (UE) 2023/2854 sui dati, che introduce norme armonizzate sull'accesso equo ai dati generati dall'utilizzo di prodotti connessi e servizi digitali.



2M+

Utenti Online

Oltre 2 miliardi di persone acquistano regolarmente online a livello globale

\$5,8T

Volume E-Commerce

Il volume globale delle transazioni e-commerce ha superato i 5,8 trilioni di dollari

3

Fonti Normative

GDPR, Codice del Consumo e Regolamento UE 2023/2854 sui dati

GDPR — Reg. UE 2016/679

Regolamento Generale sulla Protezione dei Dati: tutela fondamentale dei dati personali dei cittadini europei

Codice del Consumo — D.Lgs. 206/2005

Disciplina consumeristica italiana: diritti e tutele nei contratti a distanza e nelle transazioni digitali

Reg. UE 2023/2854 sui Dati

Norme armonizzate sull'accesso equo ai dati generati da prodotti connessi e servizi digitali

Commercio elettronico D.Lgs. 70/2023

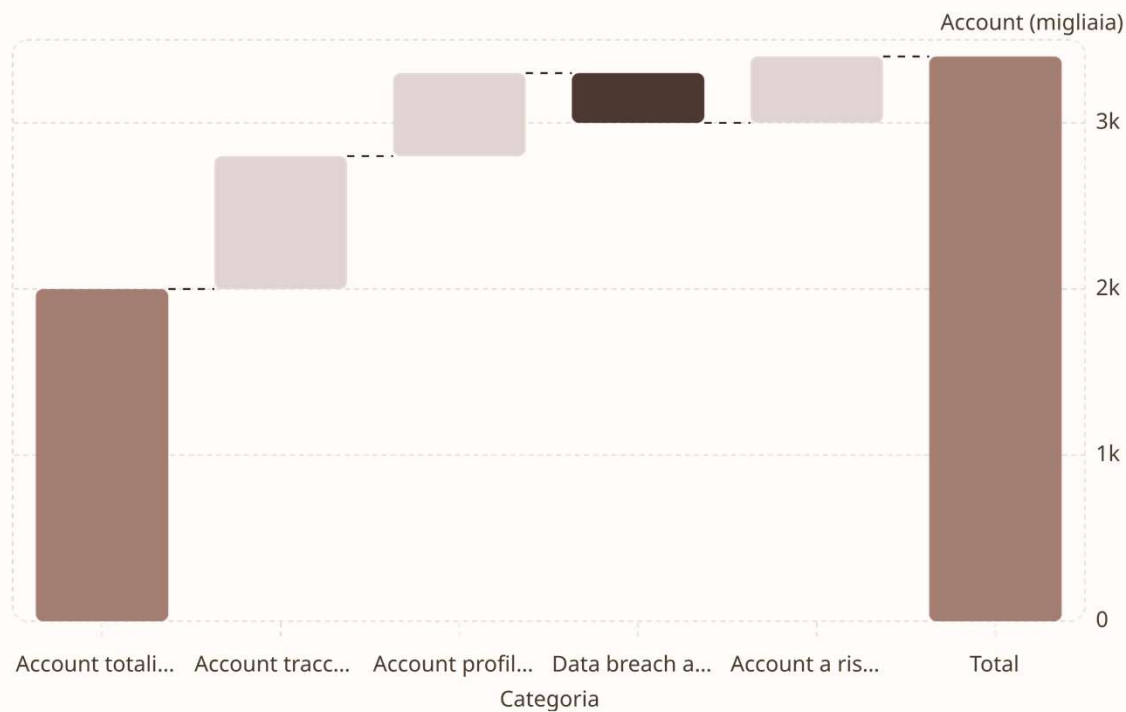
Disciplina gli obblighi informative Precontrattuali nei contratti conclusi per via telematica

Servizi di pagamento D.Lgs. 11/2010

Disciplina i servizi di pagamento, garantendo la sicurezza, la trasparenza e la tutela degli utenti nelle operazioni di pagamento

La Complicazione: Il Prezzo Nascosto dell'E-Commerce

I dati personali sono diventati la vera moneta di scambio del web. Ogni transazione online genera un flusso di informazioni che, se non adeguatamente protette, possono essere sfruttate per profilare i consumatori o cadere in mani criminali. Il rischio crescente di data breach colpisce milioni di account ogni anno.



Le Minacce Principali

Il consumatore digitale è esposto a rischi concreti che spesso sottovaluta al momento dell'acquisto.

Tracking Invisibile

Ogni clic viene tracciato per profilare il comportamento d'acquisto senza che l'utente ne sia pienamente consapevole

Data Breach

Milioni di account vengono violati ogni anno, esponendo dati personali e finanziari degli utenti

Dati come Moneta

I dati personali sono diventati la vera valuta di scambio del web: ogni acquisto genera informazioni preziose

Profilazione comportamentale

I dati raccolti vengono utilizzati per creare profili dettagliati degli utenti e personalizzare offerte commerciali

Assenza di consenso informato

Spesso gli utenti non sanno esattamente quali dati vengono raccolti e come verranno utilizzati dalle piattaforme

Vulnerabilità sistemiche

Le infrastrutture digitali presentano falle di sicurezza che possono essere sfruttate da attori malevoli

Impatto economico crescente

Le frodi online e i data breach generano perdite economiche miliardarie a livello globale ogni anno

NORMATIVA

Il Peso della Legge: Il GDPR come Scudo

Il Regolamento Generale sulla Protezione dei Dati (GDPR) rappresenta il punto di svolta europeo nella tutela della privacy. Le aziende non possono più ignorare il consenso informato e devono garantire trasparenza assoluta su chi possiede i dati degli utenti.

Regolamento UE 2016/679

Il GDPR stabilisce le regole fondamentali per il trattamento dei dati personali, imponendo obblighi precisi a titolari e responsabili del trattamento in tutta l'Unione Europea

Sanzioni Pesanti

Le aziende non possono più ignorare il consenso informato: le violazioni del GDPR possono comportare sanzioni amministrative fino al 4% del fatturato mondiale annuo

Trasparenza Obbligatoria

L'utente deve sapere esattamente chi possiede i suoi dati, per quali finalità vengono trattati e per quanto tempo saranno conservati, secondo l'art. 13 del GDPR

Accountability

Il GDPR impone ai titolari del trattamento una valutazione di risk assessment sui dati trattati e la garanzia di accountability nei confronti degli interessati

Il principio di trasparenza è ulteriormente declinato dal considerando 39 del GDPR, che esige un linguaggio semplice e chiaro. In ambito digitale, il Garante per la protezione dei dati personali ha precisato che una modalità appropriata è la strutturazione dell'informativa su più livelli (c.d. layered notice), con una prima informativa sintetica in forma di banner sulla home page, e la possibilità di approfondimento progressivo.

RISCHI

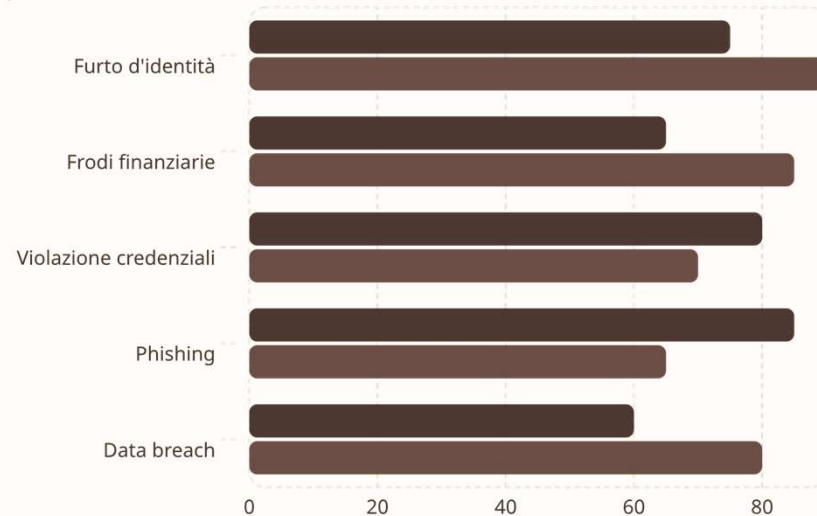
I Vulnerabili: Quando i Dati Diventano Pericolo

Le conseguenze di una falla nella sicurezza dei dati possono essere devastanti per i consumatori, sia dal punto di vista economico che psicologico. La perdita di fiducia verso i brand online è uno dei danni più difficili da recuperare.

■ Frequenza (indice)

■ Impatto percepito

Tipo di rischio



Le Conseguenze Dirette

- **Furto di identità e frodi finanziarie:** le conseguenze dirette di una falla nella sicurezza possono includere l'utilizzo non autorizzato di credenziali bancarie e dati personali
- **Vulnerabilità dei pagamenti mobili:** l'esposizione delle credenziali bancarie nei sistemi di pagamento digitale rappresenta un rischio crescente
- **Impatto psicologico:** la perdita di fiducia del consumatore verso i brand online è uno dei danni più difficili da recuperare dopo un incidente di sicurezza
- **Responsabilità dell'utente:** La comunicazione volontaria di credenziali e codici OTP può integrare colpa grave dell'utente ex art. 7 D.Lgs. 11/2010, con possibile riduzione o esclusione del rimborso; tuttavia, il PSP resta onerato di provare la corretta esecuzione dell'operazione e l'adozione di tutte le misure di sicurezza, anche nei casi di frode perpetrata con tecniche di spoofing.

●●●●● 80%

Degli utenti teme la violazione dei propri dati personali durante gli acquisti online

●●●●● 60%

Delle violazioni dei dati coinvolge credenziali di pagamento o dati bancari

●●●●● 35%

Dei consumatori abbandona un brand dopo una violazione dei dati personali

La Risoluzione Parte 1: Standard di Sicurezza Aziendali

Il GDPR impone ai titolari del trattamento di mettere in atto misure tecniche e organizzative adeguate al rischio. Nel settore dei servizi di pagamento online, la giurisprudenza ha confermato che i prestatori di servizi di pagamento (PSP) sono i soggetti più idonei a investire risorse per prevenire i rischi connessi alla trasmissione del consenso.



Protocolli HTTPS e SSL

Implementazione obbligatoria su ogni transazione per garantire la cifratura dei dati scambiati tra utente e piattaforma



Autenticazione a Due Fattori (2FA)

Adozione obbligatoria per proteggere gli accessi agli account e ai servizi di pagamento online



Minimizzazione dei Dati

Raccogliere solo le informazioni strettamente necessarie alla vendita, nel rispetto del principio di minimizzazione del GDPR



Misure Tecniche Adeguate

L'art. 32 del GDPR obbliga a pseudonimizzazione, cifratura e procedure di test periodici dell'efficacia delle misure di sicurezza

Autenticazione 2FA
Accesso utenti con doppia verifica.

Minimizzazione Dati
Raccogliere solo informazioni necessarie.

Crittografia HTTPS
Tutte le transazioni con SSL/TLS.

Test & Responsabilità
Verifiche periodiche e responsabilità chiare.

L'art. 32 del GDPR obbliga il titolare e il responsabile del trattamento a mettere in atto misure tecniche e organizzative adeguate al rischio, tra cui: pseudonimizzazione e cifratura, capacità di assicurare riservatezza, integrità e disponibilità dei sistemi, procedure di test periodici dell'efficacia delle misure.

Tuttavia, la responsabilità del PSP può essere ridotta o esclusa ove dimostri non solo l'adozione dell'autenticazione forte (SCA), ma altresì che l'operazione non ha subito malfunzionamenti e che il danno è causalmente riconducibile in via esclusiva alla condotta gravemente colposa dell'utente (art. 10 D.Lgs. 11/2010).

La Risoluzione Parte 2: L'Etica dell'Algoritmo

La protezione dei dati non è solo un obbligo legale, ma una scelta strategica che distingue le aziende responsabili. I consumatori scelgono sempre più spesso chi dimostra di proteggere la loro privacy.



Privacy by Design

Integrare la protezione dei dati fin dalla fase di sviluppo del sito e dei servizi digitali, non come aggiunta successiva



Trasparenza Radicale

Comunicare in modo semplice e comprensibile come vengono usati i dati di profilazione, nel rispetto del considerando 39 del GDPR



Etica come Vantaggio Competitivo

I clienti scelgono chi protegge la loro privacy: la tutela dei dati diventa un fattore di differenziazione sul mercato



Consenso Informato

Il consenso è irrimediabilmente viziato in assenza di un'informativa completa: un trattamento senza adeguata informativa è privo di base giuridica

- ❑ I tempi di conservazione devono essere definiti con sufficiente precisione: una conservazione per «i tempi strettamente necessari» senza ulteriore specificazione è stata ritenuta inidonea dal Garante Privacy, in quanto comprime notevolmente il controllo dell'interessato.
Art. 5, par. 1, lett. e) GDPR (principio di "limitazione della conservazione") e all'art. 25 GDPR (privacy by design e by default), che costituisce il fondamento normativo diretto dell'affermazione.

Strumenti per l'Utente: Difendersi nel Cyberspazio

La disciplina non è unilaterale: anche in capo agli utenti gravano obblighi di diligenza, in particolare quanto alla custodia delle credenziali di accesso ai servizi di pagamento online. L'art. 7 del D.Lgs. n. 11/2010 prescrive che l'utente utilizzi lo strumento di pagamento in conformità ai termini contrattuali e comunichi senza indugio al PSP lo smarrimento o l'uso non autorizzato dello strumento.

Art. 12 D.Lgs. 11/2010, che disciplina la distribuzione delle perdite tra utente e PSP in caso di operazioni non autorizzate, e in particolare:

- ☐ il comma 2-bis (esonero dell'utente in assenza di SCA da parte del PSP);
- ☐ il comma 3 (limite massimo di €50 per perdite da furto/smarrimento in assenza di dolo o colpa grave);
- ☐ il comma 4 (responsabilità integrale dell'utente in caso di dolo o colpa grave).

Il consenso dell'interessato costituisce una fattispecie complessa: esso è irrimediabilmente viziato in assenza di un'informativa completa e adeguata sul trattamento.



Password Manager Crittografati

Gestione consapevole delle password tramite strumenti sicuri che generano e conservano credenziali complesse



Pagamenti Protetti

Utilizzo di carte di pagamento virtuali o sistemi come PayPal e Apple Pay per limitare l'esposizione dei dati bancari



Revisione Periodica Privacy

Abitudine alla revisione periodica delle impostazioni di privacy sui portali e-commerce e aggiornamento delle preferenze



Custodia delle Credenziali

Non comunicare mai a terzi credenziali e codici OTP: tale condotta è stata qualificata come comportamento incauto dalla giurisprudenza

PROSPETTIVE

Il Futuro: Verso un Web Decentralizzato e Sicuro

Diritti dell'Interessato

L'art. 15 del GDPR attribuisce il diritto di accesso ai dati personali; l'art. 17 codifica il diritto alla cancellazione; l'art. 20 garantisce la portabilità dei dati.

Il Regolamento (UE) 2023/2854 rafforza il diritto di accesso ai dati generati da prodotti connessi, prevedendo che siano messi a disposizione «senza indebito ritardo, gratuitamente, in un formato completo, strutturato e leggibile da dispositivo automatico».

In caso di risoluzione del contratto, l'art. 135-undevicies del Codice del Consumo impone al professionista di rispettare gli obblighi GDPR e di astenersi dall'utilizzare i contenuti forniti dal consumatore.

Identità Digitale Sovrana

Controllo utente sui propri dati

Evoluzione Normativa

Regole aggiornate per equità

Intelligenza Artificiale

Prevenzione frodi in tempo reale

Ecosistema Digitale Equo

Bilancia tra imprese e consumatori



Identità Digitale Sovrana

L'avvento di nuove tecnologie per l'identità digitale sovrana permette agli utenti di controllare direttamente i propri dati



AI Anti-Frode

L'intelligenza artificiale applicata alla prevenzione delle frodi in tempo reale trasforma la sicurezza delle transazioni digitali



Evoluzione Normativa

La continua evoluzione normativa verso un ecosistema digitale più equo, con il Regolamento UE 2023/2854 che si affianca al GDPR



Bilanciamento Dinamico

Un sistema di tutele fondato sul bilanciamento tra protezione dei dati, diritti economici del consumatore e esigenze operative delle imprese

Conclusioni: Responsabilità Condivisa

Il sistema di tutele in materia di acquisti online e privacy si fonda su un bilanciamento dinamico tra interessi contrapposti: da un lato, la protezione dei dati personali e dei diritti economici del consumatore; dall'altro, le esigenze operative delle imprese e la libertà di informazione.

Le imprese sono tenute a un approccio proattivo e documentale (privacy by design e by default), con obblighi di trasparenza che si estendono all'intera catena del trattamento. I consumatori, a loro volta, sono titolari di un ventaglio articolato di diritti azionabili - accesso, cancellazione, portabilità, recesso — la cui effettività è garantita tanto in sede amministrativa (Garante Privacy) quanto in sede giurisdizionale.

Responsabilità delle Imprese

Proteggere la privacy è una responsabilità congiunta: le aziende devono adottare un approccio proattivo (privacy by design e by default), garantire trasparenza e rispettare gli obblighi derivanti dal GDPR e dal Codice del Consumo

E-Commerce Sicuro

Un e-commerce sicuro è la base per la crescita sostenibile del mercato: investire in sicurezza e trasparenza genera fiducia e fidelizzazione dei consumatori nel lungo periodo

Call to Action

Implementare la cultura della protezione dati oggi per garantire la fiducia di domani: la tutela della privacy è un investimento strategico, non un costo operativo

Proteggere la privacy è una responsabilità condivisa tra aziende e consumatori. Solo attraverso un impegno congiunto è possibile costruire un ecosistema digitale sicuro, equo e sostenibile per tutti gli attori del mercato.