Impatto del Framework normativo sull’e-commerce



Il settore dell’e-commerce ha registrato una crescita esponenziale negli ultimi anni, trainato dall’adozione massiva del digitale e da un cambiamento radicale nei comportamenti dei consumatori. Tuttavia, con questa espansione è diventata sempre più evidente la necessità di un framework normativo solido, che garantisca sicurezza, trasparenza e fiducia per tutti gli attori coinvolti: dai consumatori alle imprese, fino agli intermediari finanziari.

In questo contesto, l’Unione Europea ha assunto un ruolo guida nel definire regolamentazioni e direttive volte a disciplinare il commercio elettronico. Normative come la **PSD2** (**Payment Services Directive 2**), il **GDPR** (**General Data Protection Regulation**), e il Digital Services Act hanno modificato in maniera significativa il panorama del commercio elettronico. Queste disposizioni non solo definiscono obblighi per le aziende, ma modellano anche l’architettura tecnica e organizzativa delle piattaforme di vendita online.

Di seguito, analizziamo allora i principali impatti di questo panorama legislativo, focalizzandoci su quattro ambiti strategici: la Strong Customer Authentication (SCA), la protezione del consumatore, la compliance ai requisiti della PSD2 e l’evoluzione nel tempo delle disposizioni legislative legate al commercio elettronico.

Protocolli di Strong Customer Authentication

Uno degli elementi centrali della normativa PSD2 è la **Strong Customer Authentication**. Questo protocollo rappresenta una

risposta concreta alla necessità di aumentare il livello di sicurezza delle transazioni online, riducendo il rischio di frodi e migliorando la fiducia dei consumatori nei sistemi digitali di pagamento.

La SCA impone che tutte le transazioni elettroniche siano validate attraverso almeno due dei seguenti tre fattori: **conoscenza (qualcosa che solo l'utente conosce)**, **possesso (qualcosa che solo l'utente possiede)** e **inerzia (qualcosa che solo l'utente è, come un'impronta digitale o un riconoscimento facciale)**. Questo approccio multifattoriale garantisce che le identità siano verificate in modo robusto prima di autorizzare una transazione, sia essa bancaria o commerciale.

Dal punto di vista tecnico, le piattaforme e-commerce hanno dovuto aggiornare le proprie interfacce di checkout, integrando soluzioni di autenticazione forte come 3D Secure 2.0. Questo ha comportato modifiche profonde all'user experience: se da una parte la sicurezza è aumentata, dall'altra alcuni clienti hanno lamentato un processo di pagamento più lungo e complesso. Tuttavia, le statistiche dimostrano che le frodi su carte non presenti (card-not-present) sono diminuite nei Paesi che hanno applicato più rigorosamente la SCA.

Le modalità con cui viene applicata l'autenticazione forte del cliente dipendono dal tipo di transazione e dal dispositivo utilizzato. Ad esempio, nelle operazioni condotte da smartphone, si assiste a un crescente utilizzo di metodi biometrici, come il riconoscimento facciale o l'impronta digitale. Allo stesso modo, le carte di pagamento possono integrare meccanismi di autenticazione a due fattori, in cui il primo livello consiste nel riconoscimento della carta e il secondo in un codice di conferma ricevuto via SMS.

Per gli esercenti digitali, l'impatto della SCA è stato duplice. In primo luogo, è stato necessario investire in nuove tecnologie e interfacciarsi con gateway di pagamento

aggiornati. In secondo luogo, è sorta la necessità di formare il personale interno e i clienti stessi, educandoli all'uso di metodi di autenticazione avanzati come le app bancarie con riconoscimento biometrico o l'autenticazione via token.

L'adozione della SCA non è però stata uniforme in Europa: alcuni Stati membri hanno applicato periodi di transizione più lunghi, mentre altri hanno adottato approcci più rigidi. Ciò ha generato una certa frammentazione nel mercato digitale europeo, costringendo molti marketplace a sviluppare sistemi flessibili, capaci di adattarsi alle diverse interpretazioni della norma.

La PSD2 contempla alcune deroghe all'obbligo di applicare la Strong Customer Authentication, valide in circostanze particolari, come ad esempio per le transazioni considerate a basso rischio ossia quando l'importo è inferiore a una soglia prestabilita oppure per i pagamenti ricorrenti effettuati verso lo stesso beneficiario.

Standard tecnici per la Consumer Protection

La protezione del consumatore è un pilastro centrale nelle politiche europee relative all'e-commerce. L'obiettivo è garantire che l'utente finale abbia accesso a informazioni chiare, veritiere e aggiornate, possa esercitare diritti come il recesso o il rimborso, e sia protetto da pratiche commerciali scorrette o da offerte ingannevoli.

Con l'introduzione di direttive come **la Consumer Rights Directive** e più recentemente il **Digital Markets Act (DMA)**, si è assistito a una codifica sempre più precisa degli obblighi informativi delle imprese online. Ad esempio, è ora obbligatorio indicare in modo trasparente i criteri utilizzati dagli algoritmi di ranking nei marketplace, così come segnalare se un prodotto è sponsorizzato o se una recensione è

verificata.

Dal punto di vista tecnico, tutto ciò ha richiesto l'introduzione di **standard e API** che permettessero di automatizzare il tracciamento delle informazioni presentate all'utente. Alcuni esempi includono i metadata strutturati utilizzati per indicizzare correttamente i prodotti sui motori di ricerca o i tag HTML previsti per segnalare la presenza di offerte promozionali.

Le piattaforme e-commerce, specialmente quelle operanti in più Stati europei, hanno dovuto adeguare i propri flussi di navigazione e checkout per consentire ai consumatori di accedere facilmente ai termini e condizioni, alle politiche di reso e ai dati relativi alla provenienza del venditore. Inoltre, i cookie banner e i meccanismi di consenso sono diventati parte integrante dell'interfaccia utente, in conformità con il GDPR.

Un altro impatto importante degli standard tecnici legati alla protezione del consumatore è la necessità di registrare e conservare le interazioni tra cliente e piattaforma. Questo non solo per finalità di audit, ma anche per garantire la tracciabilità in caso di contenzioso. Molte aziende hanno adottato logiche di versioning sui contenuti contrattuali, conservando copia delle condizioni accettate da ciascun utente al momento dell'acquisto.

In sintesi, gli standard tecnici per la consumer protection si traducono in requisiti pratici di sviluppo software, **UX design** e gestione del ciclo di vita dei contenuti. Questi aspetti, se ben implementati, non solo evitano sanzioni amministrative, ma diventano anche un vantaggio competitivo in termini di affidabilità percepita e tasso di conversione.

Framework normativo PSD2: requisiti tecnici per le piattaforme di pagamento

La **Direttiva UE 2015/2366 PSD2** (Payment Services Directive 2) ha rivoluzionato il mondo delle transazioni digitali. Oltre alla Strong Customer Authentication, essa introduce il concetto di "open banking", ossia la possibilità per terze parti autorizzate (TPP) di accedere, con il consenso dell'utente, ai dati dei conti bancari e di avviare pagamenti direttamente. In Italia è ufficialmente operativa dal 14 settembre 2019 e ha condotto a nuovi standard di autenticazione e sicurezza per autorizzare le operazioni bancarie.

La normativa ha introdotto tre principali tipologie di servizi:

1. **Servizio di informazione sui conti (Account Information Service)**: offre agli utenti la possibilità di visualizzare il saldo e i movimenti dei propri conti correnti tramite applicazioni di terze parti, differenti rispetto alle piattaforme bancarie tradizionali.
2. **Servizio di inizio pagamento (Payment Initiation Service)**: consente ai clienti di disporre pagamenti direttamente dal proprio conto, senza passare per carte di credito, utilizzando strumenti digitali che si interfacciano in modo diretto con il conto bancario.
3. **Servizio di emissione carte (Card Issuing Service)**: permette l'utilizzo di carte di pagamento fornite da operatori diversi dalla propria banca, che funzionano come un Bancomat tradizionale, ma con accesso diretto al conto corrente dell'utente.

Questa apertura ha portato all'emergere di nuovi attori nel panorama e-commerce, come i Payment Initiation Service

Providers (PISP) e gli Account Information Service Providers (AISP), che offrono servizi innovativi per l'acquisto online e la gestione finanziaria. Ad esempio, molti marketplace oggi permettono di pagare direttamente da conto a conto, evitando l'uso delle carte di credito tradizionali e riducendo le commissioni.

Per essere conformi alla PSD2, i sistemi di pagamento del commercio elettronico devono implementare API standardizzate (in genere definite dall'European Banking Authority) e protocolli sicuri di autorizzazione come OAuth 2.0. Queste tecnologie devono essere integrate nei payment gateway e nei back-end delle piattaforme, il che spesso richiede una revisione dell'architettura software e una stretta collaborazione con le banche partner.

Dal punto di vista legale, la PSD2 impone anche l'adozione di procedure di **gestione dei consensi**, di logging sicuro e di auditing degli accessi. Ciò comporta l'implementazione di strumenti avanzati di identity management e di sistemi di monitoraggio delle frodi in tempo reale.

Una corretta implementazione della compliance PSD2 è oggi un indicatore di maturità tecnologica e di affidabilità per le aziende e-commerce. Inoltre, consente l'introduzione di servizi a valore aggiunto come il pagamento rateale istantaneo, il checkout intelligente e la gestione dinamica del credito.

Tuttavia, non tutte le aziende sono riuscite a adattarsi con la stessa rapidità. Le PMI, in particolare, hanno spesso subito ritardi nell'adeguamento per via dei costi di sviluppo e della complessità normativa. Questo ha favorito la nascita di soluzioni **white-label** e **API-as-a-service** che consentono anche ai player più piccoli di restare competitivi sul mercato. A tal proposito, a partire dal 14 settembre 2020, gli istituti bancari sono stati tenuti a rendere accessibili, tramite API (Application Programming Interface), determinati

dati relativi ai conti correnti e alle operazioni di pagamento dei propri clienti, esclusivamente a soggetti terzi autorizzati e previo esplicito consenso da parte del cliente, nel rispetto delle disposizioni previste dal GDPR.

Evolution pattern delle normative e-commerce

L'ambiente normativo che regola la vendita online non è statico, ma evolve in risposta ai cambiamenti tecnologici, economici e sociali. I cosiddetti "evolution pattern" delle disposizioni legislative rappresentano proprio questa capacità di adattamento progressivo del diritto alle nuove forme di interazione digitale.

Uno degli esempi più evidenti è l'introduzione del **Digital Services Act** (DSA) e del **Digital Markets Act** (DMA), che mirano a regolamentare in modo più efficace le grandi piattaforme online, definite come "**gatekeepers**". Questi atti legislativi introducono obblighi di trasparenza algoritmica, prevenzione della disinformazione e gestione responsabile dei contenuti.

Con il DSA e il DMA, l'Unione Europea inaugura una nuova stagione di regolazione proattiva, rivolta non più al singolo attore, ma all'intero ecosistema. I gatekeeper ovvero le piattaforme online che mediano una parte significativa del traffico digitale sono soggetti a obblighi specifici:

- **Trasparenza sugli algoritmi**: devono spiegare il funzionamento dei sistemi di raccomandazione.
- **Rimozione dei contenuti illegali**: con meccanismi più rapidi e controllabili da parte delle autorità.
- **Limitazione delle pratiche discriminatorie** nei confronti dei venditori terzi presenti sui marketplace.

Per il settore e-commerce, ciò significa l'obbligo di dotarsi di **strumenti di compliance avanzata**: dai filtri di contenuti

all’audit algoritmico, fino a sistemi antifrode e processi di verifica delle identità. L’obiettivo non è solo la conformità, ma la costruzione di una **filiera digitale più affidabile e verificabile**.

L’impatto sul commercio elettronico è duplice. Da un lato, aumenta la pressione sulle piattaforme per sviluppare sistemi di moderazione e controllo più sofisticati. Dall’altro, si incentiva l’adozione di pratiche responsabili nella gestione dei dati, della pubblicità e del trattamento delle recensioni degli utenti.

Un altro ambito in forte evoluzione è quello legato alla sostenibilità e alla **duty of care** nella supply chain digitale, dove cresce l’esigenza per le aziende e-commerce di garantire la **responsabilità ambientale e sociale** lungo tutta la catena del valore, adottando strumenti di **monitoraggio avanzato**, criteri di **due diligence** e sistemi di **rendicontazione ESG**, in risposta sia alla crescente attenzione dei consumatori, sia alle nuove disposizioni europee in materia di trasparenza e accountability. Le nuove normative in discussione – come quelle legate al **Green Deal europeo** o alla **Corporate Sustainability Due Diligence Directive (CSDDD)** – introducono principi di responsabilità estesa per i venditori online:

- **Tracciabilità ambientale e sociale** dei prodotti lungo tutta la catena di approvvigionamento;
- **Reportistica ESG (Environmental, Social, Governance) obbligatoria**, anche per PMI che operano su piattaforme internazionali;
- **Trasparenza nei processi produttivi** e negli standard adottati (es. certificazioni ambientali o di lavoro etico).

Tali requisiti comportano l’adozione di strumenti digitali evoluti per la **supply chain governance**, come i registri distribuiti (blockchain), o i **digital passport** dei prodotti.

Anche il settore delle criptovalute e dei pagamenti decentralizzati è oggetto di nuove normative, come il **Regolamento MiCA** (Markets in Crypto-Assets), che influenzerà sempre più i gateway di pagamento che vogliono accettare asset digitali. Per gli operatori e-commerce, ciò implica che l'accettazione di criptovalute come mezzo di pagamento dovrà avvenire solo attraverso **intermediari regolamentati**, con sistemi di **identificazione del cliente (KYC)**, **prevenzione del riciclaggio** e **custodia sicura degli asset**. L'interoperabilità tra il mondo fiat e crypto diventa dunque una questione legislativa, oltre che tecnica.

Infine, l'evoluzione normativa è sempre più orientata al dialogo con l'innovazione tecnologica. Si osserva una crescente interazione tra regolatori, sviluppatori e operatori del mercato, che porta alla nascita di sandbox regolamentari e framework flessibili come i **Digital Operational Resilience Act (DORA)**, pensati per gestire i rischi operativi nelle infrastrutture digitali critiche. L'obiettivo è permettere alle imprese di testare soluzioni innovative in ambienti controllati, sotto la supervisione delle autorità. DORA rappresenta un modello avanzato di **regolazione preventiva**, non più incentrata su sanzioni ex post, ma su requisiti di robustezza e reattività continua.

Conclusioni

L'impatto del framework normativo sull'e-commerce è profondo e multiforme. Le regolamentazioni non sono semplicemente vincoli da rispettare, ma leve strategiche che orientano lo sviluppo tecnologico, la progettazione dell'esperienza utente e la gestione del rischio.

Dall'autenticazione forte alle API bancarie, dagli standard informativi per la protezione del consumatore ai modelli evolutivi della regolamentazione, ogni aspetto del commercio elettronico è oggi influenzato da requisiti legislativi sempre

più articolati.

Comprendere e anticipare queste dinamiche rappresenta non solo un vantaggio competitivo, ma anche una necessità per chi vuole operare in modo sostenibile e conforme nel complesso scenario digitale attuale.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/framework-normativo/