

BROWSER E PRIVACY

Il consenso online diventa automatico: cosa cambia in Europa

Home > Sicurezza Digitale > Privacy



Partecipa al dibattito 

Il Digital Omnibus UE mantiene l'impianto del GDPR ma sposta l'asse sul consenso "machine-readable". La standardizzazione promette semplificazione, ma apre problemi di autenticità, prova e attribuzione. Tra bot, logging e standard, la libertà informazionale richiede nuove garanzie

Pubblicato il 19 feb 2026

Francesca Niola

Research Fellow Legal manager @ Aisma srl



Nel nuovo assetto europeo, il **consenso machine-readable** promette scelte più semplici e interoperabili, ma sposta il baricentro della tutela sul terreno della prova, dell'integrità tecnica e dell'attribuzione della volontà lungo la filiera digitale.



Un clic per dire sì o no: come cambia il consenso col Digital Omnibus

11 Febbraio 2026

[Indice degli argomenti](#) ▾

Omnibus digitale UE e svolta del consenso machine-readable

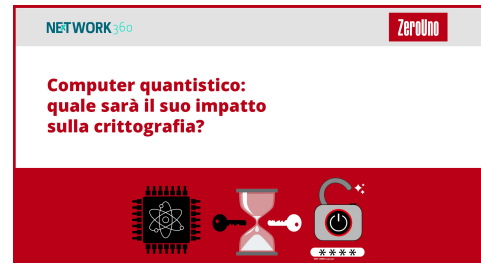
Nel settembre 2025 la **Commissione europea** ha messo in circolo il **pacchetto Digital Omnibus** che tratta la semplificazione come tecnica di governo dell'intero spazio normativo dei dati: un testo che **conserva l'architettura formale del GDPR** e, al tempo stesso, ne sposta l'asse operativo tramite interventi selettivi su definizioni, basi di liceità, trasparenza, decisione automatizzata, incident reporting, **raccordo con NIS2** e con l'ecosistema dell'**identità digitale** europea. In questa cornice, la novità che merita una lente propria riguarda il **consenso**, o meglio la sua trasformazione in segnale standardizzato, traducibile in forma automatica e **"machine-readable"**: una scelta giuridica che tocca la grammatica stessa della **libertà informazionale**, poiché converte un atto personale,

contestuale e spesso controverso in un'istruzione che viaggia tra browser, sistemi operativi, interfacce e registri.

★ EGUIDE

Sveliamo la potenza della Crittografia Quantistica: tutti i segreti per proteggere la tua azienda!

Gestione Dati # Backup



Scelta una volta, effetti molte volte: la promessa di razionalità

Il cuore concettuale sta in una promessa di razionalità: se l'utente manifesta accettazione, rifiuto, opposizione tramite mezzi automatizzati e leggibili a macchina, le interfacce online devono saper interpretare quel segnale e rispettarlo; lo stesso impianto invoca norme armonizzate, presunzioni di conformità, mandato agli organismi di standardizzazione, ed eventuale intervento della **Commissione** tramite atto delegato sui fornitori di browser e sui soggetti che definiscono regole per applicazioni software che raccolgono dati tramite **apparecchiature terminali**, qualora il mercato offra soluzioni giudicate insufficienti.

Il disegno affonda in un'idea di "scelta una volta, effetti molte volte", imparentata, sul piano della tecnica amministrativa, con il principio "segnala una volta, condividi molte" costruito per la notifica degli incidenti attraverso un punto di ingresso unico. Il consenso, in tale logica, assume la forma di flusso: un **token giuridico** che attraversa soggetti diversi e che pretende obbedienza da parte di infrastrutture private.

Prova del consenso e autenticità: il nodo che cambia il GDPR

Qui nasce il problema della **prova di autenticità**. Nel **GDPR** la prova del consenso grava sul titolare, e la regola conserva un senso intuitivo finché il consenso resta connesso a un'interazione identificabile: un modulo, una schermata, un **log** locale, una sequenza che conserva tracce leggibili anche per un giudice.

Nel modello **“machine-readable”** il titolare riceve un segnale che proviene da uno strato intermedio, spesso controllato da terzi: **browser, sistema operativo, estensione, app store, impostazioni di default, strumenti di gestione delle preferenze**. Il consenso cessa di essere soltanto un contenuto informativo e diventa un **artefatto tecnico**.

Ogni artefatto tecnico ammette contraffazioni, repliche, alterazioni, uso seriale, automazione. E nel capitalismo delle interazioni, l'automazione possiede già i suoi operai invisibili: **bot** che simulano utenti, **click-farm** che monetizzano gesto e tempo, reti di traffico artificiale che trasformano il “sì” e il “no” in materia prima.

Replay e integrità del vettore: quando basta conquistare il canale

Il passaggio decisivo, dunque, riguarda la **genuinità della scelta**. Un segnale standardizzato, per definizione, riduce la varietà del mondo a un set di codici. Tale riduzione produce efficienza, tuttavia porta con sé un effetto collaterale: la scelta diventa riproducibile.

Nel lessico della sicurezza si direbbe **“replay”**: lo stesso segnale può essere ripetuto, trasferito, riutilizzato, talvolta in modo coerente con la volontà dell'utente, talvolta per finalità estranee. La contraffazione del consenso non richiede la conquista della mente, basta la conquista del canale. Il diritto, in tale scenario, smette di interrogare soltanto il contenuto della volontà e deve misurare l'**integrità del vettore**.

Rilievo costituzionale e art. 8 Carta UE: controllo e intelligibilità

Questa torsione assume rilievo costituzionale nel senso pieno del termine, poiché l'**art. 8 della Carta UE**, insieme al principio di autonomia personale che attraversa l'intero edificio dei diritti, domanda che il trattamento dei dati resti ancorato a forme intelligibili di controllo.

L'intelligibilità, qui, riguarda anche la prova: la libertà resta parola astratta quando l'ordinamento perde strumenti affidabili per distinguere l'atto umano dall'atto simulato. La bozza stessa, con l'insistenza su **standard** e **presunzioni di conformità**, ammette implicitamente che la validità giuridica, nel digitale, dipende dalla qualità dei dispositivi di attuazione.

Attribuzione della scelta e logging: il diritto probatorio entra nel browser

Una prima linea di frizione riguarda l'**attribuzione della scelta**. Il segnale "**machine-readable**" può provenire da impostazioni generali del browser, da preferenze importate, da configurazioni consigliate, da soluzioni preimpostate dal produttore, da pacchetti di privacy settings creati da soggetti terzi. In tale catena, la domanda "chi ha scelto" perde immediatezza.

Il titolare potrà invocare il segnale come prova di un consenso o come prova di un rifiuto; l'interessato potrà contestarne la paternità; l'autorità dovrà ricostruire la genealogia del token. La disputa, spesso, ruoterà attorno a **log** e **metadati**. Qui la questione "**logging**" smette di essere un dettaglio tecnico e diventa diritto probatorio europeo.

Infrastrutture di obbedienza e analogia eIDAS: firme, timestamp, audit trail

Una seconda linea concerne l'**integrità del segnale**. La proposta attribuisce alle interfacce il dovere di interpretare e rispettare indicazioni automatizzate; attribuisce agli **standard armonizzati** la funzione di ponte tra tecnica e legalità; attribuisce alla **Commissione** un potere di intervento sul mercato dei browser e dei sistemi operativi. L'insieme costruisce una nuova categoria di "**infrastrutture di obbedienza**", nelle quali la conformità giuridica dipende dalla correttezza di implementazioni software. In tale ambiente, l'anti-contraffazione richiede strumenti simili a quelli che l'ordinamento già conosce per altri oggetti normativamente sensibili: **firme elettroniche, marche temporali**, attestazioni di origine, registri di eventi, **audit trail**.

L'analogia con l'eIDAS appare immediata: il diritto europeo dispone di una tradizione tecnica della fiducia, basata su servizi qualificati, catene di certificazione, **timestamp**, responsabilità del prestatore. Il consenso "**machine-readable**" chiede una grammatica affine, poiché il suo valore giuridico dipende dalla possibilità di dimostrare che un determinato segnale corrisponde a un determinato atto, in un determinato contesto, in un determinato momento.

Garanzia e sostenibilità: perché eIDAS non può diventare ogni click

Eppure, la trasposizione di quel modello incontra una resistenza strutturale: il consenso opera di regola in massa, nel quotidiano, su miliardi di eventi, mentre gli strumenti **eIDAS** nascono per atti puntuali, densi, spesso solennizzati.

La semplificazione invocata dal pacchetto tende a ridurre attrito e costi di conformità; una "consentizzazione" eIDAS di ogni click introdurrebbe una burocrazia tecnica pervasiva. Qui il giurista costituzionalista incontra una dialettica classica: **garanzia e sostenibilità**, intensità della prova e governabilità del sistema.

La soluzione, allora, richiede una scala intermedia: attestazioni leggere, ma robuste; tracciamenti minimizzati, ma sufficienti; **audit** selettivi, ma incisivi.

Accountability triangolare: titolare, intermediario, standard setter

L'anti-contraffazione del consenso implica anche un tema di **accountability** in senso forte. Il **GDPR** conosce l'accountability come principio organizzativo: responsabilità dimostrabile, misure adeguate, capacità di rendere conto.

Nel modello "**machine-readable**" l'accountability si sposta verso un triangolo: titolare, intermediario tecnologico, **standard setter**. Il titolare resta responsabile verso l'interessato; l'intermediario diventa produttore di condizioni di validità; lo standard setter produce i parametri che attivano presunzioni di conformità.

Questo triangolo richiede un diritto della prova che distribuisca oneri e poteri in modo coerente, altrimenti la responsabilità si trasforma in retorica contabile: il titolare "si affida al browser", il browser "si affida allo standard", lo standard "si affida alla presunzione", e l'interessato resta con un atto giuridico diventato opaco.

Media, pubblicità e potere: il consenso come regolazione di filiera

La bozza offre un indizio rivelatore: l'eccezione prevista per i fornitori di servizi di media, motivata con il ruolo degli introiti pubblicitari per il giornalismo indipendente, e con la possibile facoltà della **Commissione** di imporre obblighi ai produttori di browser e ad attori del mercato mobile per consentire la gestione e la comunicazione automatica delle preferenze.

In un testo che parla la lingua della semplificazione, questa clausola parla la lingua del potere: segnala che la disciplina del consenso diventa anche disciplina di equilibri economici e di architetture informative. Il consenso, per via indiretta, smette di essere solo tutela dell'interessato e diventa regolazione della filiera pubblicitaria, del pluralismo informativo, delle economie della piattaforma.

Manipolazione di massa: bot, click-farm e industrializzazione della scelta

Qui il tema dell'autenticità acquista un secondo volto: autenticità come resistenza alla **manipolazione di massa**. Bot e click-farm agiscono come dispositivi di distorsione della volontà collettiva, perché producono segnali che le infrastrutture trattano come scelte reali.

Il consenso, in forma di segnale, diventa una superficie d'attacco anche per strategie di influenza: campagne che spingono configurazioni predefinite, pacchetti di impostazioni che favoriscono certe basi di trattamento, estensioni che promettono protezione e poi instradano preferenze in modo opportunistico. In termini costituzionali, la questione supera l'individuo e tocca l'ecosistema: la **libertà informazionale** perde spessore quando la sua espressione viene industrializzata.

Quattro requisiti anti-contraffazione: contestualità, canale, attribuzione, audit

L'anti-contraffazione, allora, richiede criteri che il diritto può articolare con precisione.

- Primo: un requisito di **"contestualità probatoria"**, cioè la capacità di collegare il segnale a un contesto di informazione sufficiente, in modo che la scelta non resti un puro bit.
- Secondo: un requisito di **"integrità del canale"**, cioè misure che riducano la possibilità di alterazione del segnale lungo la catena tecnica.
- Terzo: un requisito di **"attribuzione controllabile"**, cioè meccanismi che consentano all'interessato di verificare le preferenze attive e la loro storia essenziale, con tracce accessibili anche in sede di reclamo.
- Quarto: un requisito di **"auditabilità"**, che permetta a autorità e terze parti qualificate di controllare implementazioni, soprattutto quando presunzioni di

conformità e standard armonizzati assegnano immunità di fatto a scelte di design.

Logging probatorio e minimizzazione: prova selettiva tra hash e tempi certi

Su questo sfondo, la nozione di **logging** cambia natura. Il logging classico registra eventi per fini di sicurezza e diagnosi; il logging del consenso assume valore di prova; il logging probatorio può trasformarsi in nuovo trattamento massivo. Il diritto deve mantenere una tensione interna: da un lato la necessità di tracce affidabili; dall'altro il principio di **minimizzazione** e la tutela contro l'accumulo indiscriminato di dati. La soluzione più coerente con la razionalità europea consiste in una prova a granularità selettiva: registrazione di elementi essenziali, uso di tecniche di **hash** e marcatura temporale, conservazione per periodi determinati, separazione funzionale tra log di sicurezza e log di prova, accesso regolato e tracciato. In tale assetto, la prova del consenso si avvicina alla prova documentale digitale, con la differenza che il documento diventa un evento.

Terminale, ePrivacy e tracciamento: il consenso come automazione del rischio

Il pacchetto, inoltre, intreccia la questione del consenso con la disciplina del trattamento "su o da **apparecchiature terminali**" e con la spinta verso la gestione delle scelte tramite impostazioni di browser e applicazioni, richiamando la storia normativa della direttiva **ePrivacy** e la proposta del 2017 sulle comunicazioni elettroniche. Qui la prova di autenticità incontra un terreno ancora più delicato: il terminale. Il terminale funge da protesi dell'identità digitale, da luogo di accumulo di preferenze, da piattaforma di estrazione di dati.

La protezione del terminale, storicamente, possiede un nucleo di "**integrità**" che va oltre la privacy in senso stretto. Il trasferimento della materia nel GDPR, con

l'allineamento delle basi e con la moltiplicazione delle possibilità giustificative, attribuisce al consenso un ruolo diverso: meno rito, più componente di un sistema di gestione del rischio e del marketing. Il segnale "machine-readable" diventa anche strumento di automazione del tracciamento, e dunque bersaglio di falsificazioni economiche.

AI Act e legittimo interesse: un segnale falsificato e gli effetti a cascata

L'intreccio con l'AI Act accentua la posta. La bozza modifica l'art. 9 in modo da riservare la protezione rafforzata ai dati che "rivelano direttamente" informazioni sensibili, e introduce una deroga per trattamenti nel contesto dello sviluppo e del funzionamento di sistemi e modelli di IA, con un regime che parla di misure tecniche e organizzative, rimozione dei dati sensibili, sforzo sproporzionato, protezione contro uso per produrre output o contro divulgazione.

La stessa bozza collega il trattamento di dati personali nel ciclo di vita dell'IA a una possibile base di **legittimo interesse**. In un universo nel quale il consenso diventa segnale e l'IA diventa infrastruttura di decisione, la contraffazione del consenso rischia di produrre effetti a cascata: un segnale falsificato può legittimare raccolte e riusi che alimentano addestramento, profilazione, scoring, e dunque decisioni con effetti giuridici significativi. Qui la prova di autenticità non tutela soltanto la libertà di essere lasciati in pace; tutela la libertà di non essere classificati sulla base di un atto attribuito in modo improprio.

Delega, standard setting e legittimazione: quando la volontà vive nel codice

Un ulteriore tratto di modernità, paradossalmente, riguarda la delega. Il testo affida molto alla standardizzazione e agli atti della **Commissione**. Il giurista costituzionalista riconosce in questa scelta una forma di normazione per infrastruttura: la regola vive nel codice, la legalità vive nel riferimento a standard,

la garanzia vive nell'audit. Tale spostamento chiede attenzione, perché la prova di autenticità del consenso diventa prova di conformità tecnica a una norma elaborata fuori dai canali politici tradizionali, pur con procedure formali.

La legittimazione democratica, in Europa, percorre anche vie tecniche; tuttavia, quando la tecnica decide la forma della volontà individuale, la densità delle garanzie richiede un controllo più esigente sui processi di standard setting, sui conflitti di interesse, sulle metriche di conformità.

Dimensione culturale: diritto alla visibilità delle preferenze e design giuridico

Il tema della contraffazione possiede, infine, una dimensione culturale: la riduzione della scelta a segnale riduce anche la pedagogia del diritto. Il banner, per quanto detestabile, costringe a un incontro, spesso brutale, con l'idea di tracciamento. Il segnale **"machine-readable"** promette discrezione: preferenze impostate una volta, interazioni più pulite, meno attrito.

Tale discrezione comporta un costo: la scelta scivola nel fondo dell'interfaccia, diventa default, diventa oggetto di ottimizzazione. In un ambiente così strutturato, l'autenticità richiede anche un diritto alla visibilità delle proprie preferenze, un diritto alla comprensione delle conseguenze, un diritto alla rettifica semplice del proprio profilo di consenso. In altre parole, l'anti-contraffazione non vive solo di crittografia e log; vive anche di un design giuridico che preservi l'atto umano come atto umano.

Verso un diritto della prova per i flussi di consenso

La bozza offre già alcuni materiali per un diritto della prova applicato ai flussi di consenso: obbligo per le interfacce di interpretare e rispettare segnali automatizzate; norme armonizzate con presunzioni di conformità; ruolo della Commissione nel richiedere standard; possibile obbligo su browser e sistemi operativi; eccezioni settoriali collegate al pluralismo informativo.

Su questa base, la riflessione giuridica può assumere un compito più sottile rispetto alla denuncia: descrivere una nuova economia della volontà, nella quale la libertà informazionale vive come oggetto tecnico e, dunque, richiede dispositivi anti-contraffazione comparabili a quelli che l'Europa ha costruito per la fiducia digitale. La posta non coincide con un dettaglio di compliance; coincide con la possibilità stessa di distinguere la persona dal suo fantasma automatizzato, nel punto in cui il diritto chiede alla persona una parola, e la macchina impara a pronunciarla al posto suo.

INFOGRAFICA

Applicare la NIS2: strategie e soluzioni per una protezione completa. Scarica ora!

 Network Security  Data protection



@RIPRODUZIONE RISERVATA

Valuta la qualità di questo articolo



Francesca Niola

Research Fellow Legal manager @ Aisma srl

Seguimi su 

Leggi anche:

- [AI per l'antiriciclaggio, ecco applicazioni e vantaggi per banche e imprese](#)
- [ChatGPT Pulse, la nostra prova: perché usarlo e perché no](#)
- [Migliorare la compliance nel telemarketing: cosa funziona e cosa no](#)



Lasciaci il tuo parere!

B *I* U

Nome

Email*

Sito web

Commenta

0 COMMENTI

WHITEPAPER

La nuova data governance nell'era dell'AI: come migliorare il processo decisionale

20 Ott 2025

WHITE PAPER

AI Act: cosa cambia per le imprese con l'entrata in vigore dei divieti e degli obblighi formativi

17 Dic 2025



Argomenti



conservazione digitale



crittografia



dati personali



eidas

Canali



Privacy



Sicurezza digitale

Con o Senza – Galaxy AI per il business

Galaxy AI

Filtra per topic



CON SENZA l'AI in ufficio?

PA mobile, i vantaggi di continuità operativa, sicurezza integrata e lavoro connesso

TECNOLOGIE

InnovAttori



L'IA alleata degli chef: così aiuta a innovare e a sprecare meno

19 Feb 2026



Tracciabilità supply chain, come Erp e cloud spingono la competitività

14 Nov 2025



Manifattura elettronica, come salvare il settore con la gestione smart degli impianti

31 Ott 2025

Cybersecurity nel manifatturiero, perché puntare sulle persone: il ruolo di policy e formazione

01 Ott 2025

AI per il lavoro in condizioni estreme, quali tecnologie scegliere

27 Ago 2025

[Vedi tutti gli approfondimenti >](#)

Articoli correlati

AI per l'antiriciclaggio, ecco applicazioni e vantaggi per banche e imprese

30 Giu 2025

di Sergio Boccadutri

Condividi 

INTELLIGENZA ARTIFICIALE

ChatGPT Pulse, la nostra prova: perché usarlo e perché no

08 Ott 2025

di Antonio Cisternino

Condividi 

WHITE PAPER

AI Act: cosa cambia per le imprese con l'entrata in vigore dei divieti e degli obblighi formativi

17 Dic 2025

Scaricalo gratis!

DOWNLOAD