CONSUMERPRO

BOOSTING PROFESSIONALS
IN CONSUMER PROTECTION

Diritti digitali

DOCUMENTO TEORICO DI BASE 2022-2023

Digital Rights - Italy
October 2022 - version 1

QUESTO MATERIALE È STATO PRODOTTO NEL CONTESTO DEL PROGETTO CONSUMER PRO, CHE È UN'INIZIATIVA DELLA COMMISSIONE EUROPEA NELL'AMBITO DEL PROGRAMMA EUROPEO PER I CONSUMATORI. IL SOSTEGNO DELLA COMMISSIONE EUROPEA NON COSTITUISCE UN'APPROVAZIONE DEL CONTENUTO CHE RIFLETTE SOLO LE OPINIONI DEGLI AUTORI. LA COMMISSIONE NON PUÒ ESSERE RITENUTA RESPONSABILE PER QUALSIASI USO CHE POSSA ESSERE FATTO DELLE INFORMAZIONI IVI CONTENUTE.

TABELLA DEI CONTENUTI

INTRODUZIONE AL DOCUMENTO TEORICO DI BASE

Caro lettore, Cara lettrice,

Questo documento teorico di base fa parte delle risorse di formazione sviluppate per Consumer Pro, un'iniziativa dell'UE che mira a rendere le organizzazioni dei consumatori e altri attori della politica dei consumatori meglio attrezzati per proteggere i consumatori nel loro paese.
L'obiettivo di questo documento è quello di fornire a voi, ai vostri team e ai vostri colleghi, informazioni utili e rilevanti sui diritti digitali. Il suo contenuto è stato preparato dagli esperti BEUC in materia di diritti digitali, da una prospettiva europea e al fine di fornire le chiavi per:

- Formare rapidamente i vostri team di professionisti;
- Trovare facilmente le informazioni pertinenti;
- Permettere al vostro personale di informare meglio i consumatori sui loro diritti, e,
- Sensibilizzare i vostri ministeri e autorità nazionali sui diritti digitali.

Questo documento teorico di base fa parte di una serie di risorse di formazione che sono destinate ad essere adattate alle specificità nazionali ove presenti. Ci sono documenti teorici complementari accessibili su richiesta o online, sui temi dei diritti digitali e dei ricorsi collettivi, in inglese e in molte altre lingue europee.

INFORMAZIONI SU CONSUMER PRO

Consumer PRO è un'iniziativa della Commissione europea nell'ambito del programma europeo per i consumatori e attuata dal BEUC - l'organizzazione europea dei consumatori. Il suo obiettivo è quello di costruire la capacità delle organizzazioni europee dei consumatori e di altri attori nella politica dei consumatori attraverso la continua formazione. Il progetto copre gli Stati membri dell'UE, l'Islanda e la Norvegia.

Per ulteriori informazioni, scrivere a *Info@consumer-pro.eu.*

La Commissione europea offre anche una formazione pratica per le PMI che vogliono capire i loro obblighi quando commerciano con i consumatori nell'UE. (ConsumerLawReady.eu).

PROTEZIONE DEI DATI

INTRODUZIONE E STORIA DELLA POLITICA DI PROTEZIONE DEI DATI DEL CONSUMATORE

La protezione delle persone fisiche in relazione al trattamento dei dati personali è un diritto fondamentale nell'Unione europea. L'**articolo 8**, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e l'**articolo 16,** paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE) stabiliscono che ogni persona ha diritto alla protezione dei dati personali che la riguardano. Inoltre, l'**articolo 7** della Carta dei diritti fondamentali afferma che ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e delle sue comunicazioni.

Il regolamento generale sulla protezione dei dati (GDPR) è la legge che regola il trattamento dei dati personali nell'UE. Richiede alle organizzazioni, sia enti pubblici che aziende, di utilizzare i dati personali dei consumatori in modo trasparente e corretto. Rafforza i diritti dei cittadini dell'Unione e si applica a tutte le organizzazioni che trattano i dati personali degli individui che si trovano nell'UE, indipendentemente da dove le organizzazioni hanno sede.

Le norme sulla ePrivacy (attualmente la direttiva ePrivacy, che è in fase di revisione) proteggono la riservatezza delle comunicazioni elettroniche e contengono anche protezioni specifiche per i consumatori contro le comunicazioni commerciali non richieste inviate tramite servizi di comunicazione elettronica.

PERCHÉ LA PROTEZIONE DEI DATI È IMPORTANTE PER I CONSUMATORI

Anche se vantaggiose per i consumatori, le tecnologie dell'informazione digitale e l'emergere di **nuovi servizi online** rappresentano **anche** una **grande sfida ai diritti fondamentali della privacy e della protezione dei dati personali**. I modelli di business che attualmente dominano il mondo digitale si basano sul tracciamento e l'analisi di ogni movimento dei consumatori. Le aziende utilizzano le informazioni che raccolgono per costruire profili di utenti, che vengono scambiati online e utilizzati per fornire pubblicità mirata ai comportamenti, ai gusti e alle preferenze dei consumatori potenziali clienti. Questi profili potrebbero anche essere usati per discriminare i consumatori e influenzare il loro comportamento. È importante assicurare che i consumatori possano rimanere in controllo dei loro dati personali e beneficiare di prodotti e servizi digitali innovativi senza dover rinunciare alla loro privacy.

PRINCIPALI SFIDE DELLA POLITICA DEI CONSUMATORI IN MATERIA DI PROTEZIONE DEI DATI

È molto difficile per i consumatori essere in grado di controllare cosa succede con i loro dati nella pratica. I loro diritti molto spesso non sono rispettati e spesso sono costretti ad accettare di rinunciare alla loro privacy se vogliono usare prodotti e servizi digitali.
I consumatori sono sotto costante sorveglianza commerciale e i loro dati personali sono sfruttati da una miriade di aziende, molte delle quali non hanno mai nemmeno sentito parlare. Le politiche sulla privacy sono vaghe, lunghe, complesse e molto difficili da capire e il consumatore non ha altra scelta che accettare. Ai consumatori viene spesso data un'illusione di controllo e nei casi in cui viene chiesto il loro consenso, questo diventa un esercizio sistematico e senza senso di "spuntare la casella".

Il GDPR doveva affrontare molti di questi problemi. Tuttavia, quasi quattro anni dopo la sua entrata in vigore, non ci sono stati cambiamenti significativi nelle pratiche commerciali. Il livello di conformità è basso in alcune aree e l'applicazione non è per il momento pienamente efficiente.

Le autorità di protezione dei dati stanno avendo difficoltà a far fronte a tutti i reclami che stanno ricevendo e la nuova architettura di applicazione, costruita intorno a un meccanismo di cooperazione e di coerenza per garantire l'interpretazione e l'applicazione coerente della legge in tutta l'UE, sta affrontando sfide ardue.

Un'altra questione, in sospeso da più di cinque anni e per la quale ancora non c'è un accordo in vista, è la riforma delle norme ePrivacy.

Queste dovrebbero integrare il GDPR e proteggere ulteriormente la riservatezza delle comunicazioni. (Per maggiori informazioni sul regolamento ePrivacy vedere la scheda informativa BEUC).

I PRINCIPALI DIRITTI E OBBLIGHI DEI CONSUMATORI

UIl GDPR richiede alle organizzazioni, sia enti pubblici che aziende, di utilizzare i dati personali dei consumatori in modo trasparente e corretto.
Contiene una serie di principi che regolano l'uso dei dati personali:

Dà anche ai consumatori una serie di diritti per garantire che possano avere il controllo dei loro dati. Tra gli altri, i consumatori hanno il diritto di:

- Essere informati, in modo chiaro e facilmente comprensibile, su come vengono utilizzati i loro dati personali. Questo deve specificare quali dati vengono utilizzati, da chi e per quali scopi;
- Accedere ai dati che le organizzazioni detengono su di loro e ottenere una copia dei dati;
- Rettificare i loro dati se sono inesatti;
- Far sì che le organizzazioni cancellino i loro dati;
- Chiedere alle organizzazioni di smettere di usare i loro dati, temporaneamente o permanentemente;
- Ricevere i loro dati in un formato comunemente usato, in modo che possano prenderli e usarli da qualche altra parte;
- Contestare decisioni automatizzate basate sui loro dati personali che li riguardano in modo significativo (ad esempio, il rifiuto di un prestito);
- Essere informati se i loro dati vengono persi o rubati;

Presentare un reclamo alla loro autorità nazionale per la protezione dei dati o citare un'azienda in tribunale.

LEGGI E REGOLAMENTI A LIVELLO EUROPEO E NAZIONALE

La Carta dei diritti fondamentali dell'UE

Regolamento (UE) 2016/679 sulla protezione delle persone fisiche in relazione al trattamento dei dati personali e sulla libera circolazione di tali dati (GDPR).

Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva sulla privacy e le comunicazioni elettroniche) - Modificata dalla direttiva 2009/136/CE

Linee guida, raccomandazioni e buone pratiche del Comitato europeo per la protezione dei dati

Pareri del garante europeo della protezione dei dati

Esempio di codice di condotta: Federazione del marketing diretto

GIURISPRUDENZA

Per un archivio delle decisioni dell'Autorità per la protezione dei dati e della Corte, così come articoli sul GDPR, visitare: www.GDPRHub.eu.

Sul portale ufficiale del diritto dell'UE: Dossier Eurlex sul GDPR. Si tratta di una lista di casi e questioni preliminari della Corte di giustizia europea che riguardano il GDPR: trovate la lista della giurisprudenza alla voce "informazioni sui documenti".

COSA POSSONO FARE I CONSUMATORI SE HANNO UN PROBLEMA?

Se il consumatore ritiene che i suoi diritti ai sensi del GDPR siano stati violati, ci sono due opzioni:

- Presentare un reclamo all'autorità nazionale per la protezione dei dati: www.garanteprivacy.it

- Presentare un'azione direttamente in tribunale contro un'azienda/organizzazione. Questo non impedisce al consumatore di presentare un reclamo presso le autorità nazionali di protezione dei dati, se lo desidera.

Inoltre, se il consumatore ritiene che l'autorità di protezione dei dati non abbia trattato correttamente il suo reclamo o se non è soddisfatto della sua risposta o se l'autorità non lo informa sullo stato di avanzamento o sul risultato, entro 3 mesi dal giorno della presentazione del reclamo, il consumatore può intentare un'azione direttamente davanti a un tribunale contro l'autorità di protezione dei dati.

Autorità pubbliche

A livello nazionale:
I ministeri nazionali incaricati della protezione dei dati (in Italia il Ministero della Giustizia), stabiliscono la politica nazionale sul tema e devono garantire l'attuazione del GDPR a livello nazionale.

Oltre alle autorità nazionali per la protezione dei dati, altri enti pubblici da considerare sono:

A livello europeo:

- La Commissione europea, che ha il compito di garantire che gli Stati membri attuino correttamente il GDPR e ha anche il potere di "attivare" alcune disposizioni del GDPR attraverso atti delegati (ad esempio per la creazione di "icone della privacy" standardizzate);
- Il Comitato europeo per la protezione dei dati (EDPB), che riunisce tutte le autorità nazionali di protezione dei dati. Il suo compito principale è quello di garantire la coerenza nell'applicazione e nell'interpretazione del GDPR;
- Il Garante europeo della protezione dei dati (GEPD), che sorveglia il rispetto dei dati personali delle persone da parte delle istituzioni dell'UE e consiglia le istituzioni in materia di protezione dei dati.

Risoluzione alternativa delle controversie (ADR)

I procedimenti extragiudiziali e altre procedure di risoluzione delle controversie tra i responsabili del trattamento e gli interessati in materia di trattamento dei dati personali possono essere stabiliti tramite codici di condotta adottati da organismi di settore (articolo 40 GDPR), fatti salvi i diritti degli interessati di presentare reclami alla loro autorità di protezione dei dati e di cercare rimedi giudiziari in tribunale.

ULTERIORI RISORSE - SCHEDE, PUBBLICAZIONI, LINK

- Sito web della Commissione europea con informazioni sul GDPR
- Biblioteca GDPR della Commissione europea - Infografiche, schede informative e altri materiali destinati a cittadini e imprese
- BEUC Factsheet - Cosa significa per te la legge europea sulla protezione dei dati?
- Rapporto BEUC - La strada lunga e tortuosa: Un caso di applicazione transfrontaliera della protezione dei dati dal punto di vista del consumatore
- AccessNow - Guida all'uso della protezione dei dati nell'UE: I vostri diritti e come esercitarli
- Agenzia dei diritti fondamentali - Manuale europeo di protezione dei dati
- Guide pubblicate dalle autorità di protezione dei dati a livello nazionale (controllate il sito web della vostra autorità nazionale di protezione dei dati)
- Fogli informativi pubblicati dal Garante europeo della protezione dei dati (GEPD)
- La storia del GDPR e un glossario (GEPD)

PIATTAFORME ONLINE

INTRODUZIONE E STORIA DELLE PIATTAFORME DI VENDITA ONLINE

I consumatori comprano sempre più servizi e prodotti online, in particolare attraverso le piattaforme.

Nei primi anni del commercio elettronico gli acquisti avvenivano principalmente su siti web di aziende che avevano anche negozi fisici nelle strade principali. Oggi, il comportamento d'acquisto dei consumatori sta cambiando radicalmente: sempre più persone ordinano servizi e prodotti attraverso marketplace online che vengono spediti ai consumatori europei direttamente da fuori dell'UE.

Gli acquisti non vengono fatti solo attraverso piattaforme di e-commerce come Amazon Marketplace, AliExpress, wish.com o eBay ma anche attraverso piattaforme di social media come Instagram.

Per esempio, nel 2017 circa 100 milioni di vendite sono state effettuate dalla Cina alla Germania. Questo dato è di 40 milioni in più rispetto al 2016. Aumenti enormi sono stati registrati anche in altri paesi europei.

Inoltre, le truffe sono in aumento per quanto riguarda i negozi web creati nell'UE da venditori che fingono di essere aziende europee, ma che in realtà stanno ordinando su piattaforme dalla Cina, e vendono questi prodotti ai consumatori per un prezzo più alto che per esempio su wish.com. Questo è stato osservato in Danimarca e in Francia.
Ci sono anche preoccupazioni molto serie che molti di questi prodotti non siano conformi alle leggi e alle norme tecniche europee che sono in atto per proteggere i diritti dei consumatori, la sicurezza, la salute e l'ambiente . Mentre i produttori e i distributori che si trovano nell'UE possono essere ritenuti responsabili della sicurezza e della conformità dei prodotti, questo spesso non è il caso dei produttori extra UE, poiché gli intermediari, cioè le piattaforme di e-commerce, negano la responsabilità della conformità.

Ci sono importanti iniziative legislative attualmente in discussione per affrontare alcuni di questi problemi, in particolare la proposta di un Digital Services Act e la proposta di un regolamento sulla sicurezza generale dei prodotti.

PERCHÉ LE PIATTAFORME SONO IMPORTANTI PER I CONSUMATORI

Fare shopping, connettersi con amici e familiari, condividere esperienze, guardare un film, ascoltare musica, leggere un libro, prenotare un viaggio, cucinare una nuova ricetta, pianificare una serata fuori, muoversi in una città, chiedere l'aiuto dei vicini e cercare informazioni sul web; questi sono solo alcuni esempi basilari di attività che milioni di consumatori svolgono ogni giorno. Per ognuna di queste attività, ci sono una o più piattaforme online che facilitano questi servizi. I consumatori hanno abbracciato l'ondata dell'economia delle piattaforme, che presenta numerosi vantaggi ma anche sfide per la protezione dei consumatori.

PRINCIPALI SFIDE RIGUARDANTI LE PIATTAFORME

In generale, quando la direttiva eCommerce è stata adottata (nel 2000), piattaforme come Google, Amazon o Booking.com erano agli inizi. Molti altri intermediari non esistevano nemmeno. Per esempio, Facebook e Shopify sono stati lanciati nel 2004. Etsy è stato fondato nel 2005; Airbnb nel 2008. Instagram, Wish e AliExpress hanno visto la luce nel 2010.

Negli ultimi 20 anni, i modelli di business di alcune di queste e altre aziende sono cambiati. Anche le dinamiche del potere di mercato sono cambiate.
Il panorama del mercato digitale europeo ha sperimentato la "*datafication*" (il trasferimento di informazioni in dati, e questo è la base dei modelli di business digitali); una moltiplicazione delle piattaforme; una proliferazione dell'economia collaborativa5; e una diversificazione dei fornitori di servizi in termini di funzioni, integrazione verticale e dimensioni. Eppure, ogni singola azienda deve giocare secondo le regole. La protezione dei consumatori non deve dipendere dalle dimensioni dell'azienda. Dopo tutto, la start-up o la PMI di oggi potrebbe diventare l'Alibaba di domani.
Molte piattaforme si sono reinventate. Alcune non si limitano più al loro ruolo iniziale di informazione o di intermediari di fiducia (per esempio le piattaforme di confronto o di classifica come Yelp) ma permettono di concludere anche transazioni sulla piattaforma. Si tratta di modelli di business che fanno rientrare la piattaforma nella categoria "marketplace", su cui si concentrano attualmente le organizzazioni di tutela dei consumatori. Questo tipo di piattaforma è definito dalla direttiva Omnibus come "un servizio che utilizza un software, compreso un sito web, parte di un sito web o un'applicazione, gestito da o per conto di un commerciante che consente ai consumatori di concludere contratti a distanza con altri commercianti o consumatori".

Detto questo, spesso il ruolo della piattaforma non si limita a consentire la conclusione di un contratto tra venditori e acquirenti, ma comprende anche altri servizi come i servizi di pagamento, i servizi di adempimento, il trattamento dei resi e la gestione dei reclami .

Altre piattaforme hanno acquisito ruoli multipli. Ci sono "*piattaforme ibride*", che possono combinare diverse funzioni di intermediazione o piattaforme integrate verticalmente. Queste ultime non agiscono solo come intermediari, ma competono anche con i commercianti, direttamente o tramite società affiliate. Per esempio, Amazon è un venditore, un mercato online, una società di cloud computing, una piattaforma di condivisione video, un editore, una società di pubblicità, un produttore di dispositivi connessi e una società di intelligenza artificiale.

Le organizzazioni dei consumatori chiedono adeguamenti del quadro legislativo per affrontare questa nuova realtà del mercato. La proposta di una legge sui servizi digitali (DSA) è un'iniziativa molto importante in questa prospettiva.

La Commissione ha presentato la proposta DSA nel dicembre 2020. Attualmente è nelle fasi finali del processo legislativo. Un accordo è atteso entro il 2022.

SFIDE E OBIETTIVI SPECIFICI

Sfida n. 1. Limitare la diffusione di una vasta gamma di contenuti illegali.
I servizi digitali sono diventati - in una certa misura - un facilitatore di diffuse violazioni del diritto dei consumatori; un flusso di entrate per la vendita di pubblicità o la promozione di prodotti pericolosi, insicuri e illegali online. Per esempio :

Un membro britannico del BEUC, ha trovato luci per l'albero di Natale vendute online che potrebbero prendere fuoco o fulminare i consumatori1

Il Consiglio dei consumatori danese ha rivelato che i cosmetici su wish.com non sono conformi al diritto comunitario

Più recentemente, sei membri del BEUC hanno scoperto che due terzi dei 250 prodotti acquistati dai marketplace online non hanno superato i test di sicurezza, con conseguenze come scosse elettriche, fuoco o soffocamento.

Sfida n. 2. Rendere chiara la differenza tra le attività del mercato online e le altre attività della piattaforma.
Il dibattito per riformare la direttiva sul commercio elettronico si sta in qualche modo concentrando su questioni come l'incitamento all'odio, i contenuti terroristici, il materiale protetto da copyright, la libertà di parola o le considerazioni sul mercato unico. Mentre queste sono questioni importanti, l'UE non dovrebbe anche perdere di vista i problemi specifici della protezione dei consumatori.
È necessario garantire che i consumatori che acquistano prodotti o servizi attraverso i marketplace online12 siano pienamente protetti.

È necessario distinguere tra la vendita di prodotti illegali e altre attività, ad esempio la pubblicazione di commenti sui social media. Mentre nel secondo caso ci sono chiare considerazioni sulla libertà di espressione, nel primo caso la questione principale in gioco è distante dal diritto alla libertà di parola, ma è piuttosto una questione legata alla sicurezza del prodotto e di protezione del consumatore.

Sfida n. 3. La direttiva eCommerce "non si applica ai fornitori di servizi stabiliti in un paese terzo" .
Alcuni fornitori stabiliti in paesi terzi stanno sfruttando le limitazioni di territorialità della direttiva - creando un campo di gioco ingiusto e ineguale.

Sfida n. 4. Il modo in cui la direttiva eCommerce regola i fornitori di hosting viene usato da alcune piattaforme - inclusi (ma non solo) i marketplace online - per proteggersi da qualsiasi responsabilità o per non intraprendere alcuna azione significativa per paura della responsabilità.

Sfida n. 5. La legislazione attuale ha delle lacune per regolare i mercati online. Poca attenzione è data all'arricchimento dei mercati online dai contenuti illegali.

Sfida n. 6. Le nuove regole possono agire come una barriera per gli Stati membri per affrontare correttamente gli obiettivi di interesse pubblico.
Per esempio, nella causa C-390/1814 , la CGUE ha stabilito che Airbnb deve essere considerato un servizio della società dell'informazione (art. 2.a) della direttiva sul commercio elettronico). Poiché la Francia non ha notificato alla Commissione una legge che richiede la licenza professionale di un agente immobiliare a società come Airbnb, non può imporre questo obbligo a Airbnb, in quanto ciò violerebbe l'articolo 3.4 b) della direttiva sul commercio elettronico. Questo caso ha dimostrato che la direttiva sul commercio elettronico, nel mettere il mercato interno al primo posto, crea problemi agli Stati membri per adottare leggi e politiche per proteggere i consumatori.
È importante però notare che la sentenza non significa che i governi non possano imporre tali misure a società come Airbnb. La CGUE è stata chiara sul fatto che l'obbligo di notifica nella direttiva eCommerce "*non ha lo scopo di impedire a uno Stato membro di adottare misure che rientrano nel proprio campo di competenza e che potrebbero incidere sulla libera prestazione di servizi, ma di impedire a uno Stato membro di interferire con la competenza, in linea di principio, dello Stato membro in cui è stabilito il fornitore del servizio della società dell'informazione interessato.*"

Sfida n. 7. Mancanza di un'adeguata supervisione e applicazione.
I mercati digitali si evolvono ad una velocità elevata e le autorità competenti non sembrano essere all'altezza, non hanno tutte le competenze o le risorse necessarie per monitorare e affrontare i problemi del mercato.

I PRINCIPALI DIRITTI E OBBLIGHI DEI CONSUMATORI IN POCHE PAROLE

La direttiva sul commercio elettronico è stata una delle pietre miliari di Internet per molto tempo. La direttiva ha stabilito il principio del paese d'origine con alcune importanti eccezioni (in particolare i contratti con i consumatori), gli obblighi fondamentali d'informazione verso i destinatari dei servizi (per esempio i consumatori), le esenzioni e le limitazioni di responsabilità per i fornitori di servizi intermediari online, tra le altre disposizioni:

- **Articolo 1 - 3: Disposizioni generali**
- **Articolo 4 - 15: Principi**

Sezione 1: Requisiti di stabilimento e di informazione
Sezione 2: Comunicazioni commerciali Sezione 3: Contratti online
Sezione 4: Responsabilità dell'intermediario

- **Articoli 16 - 20: Attuazione**
- **Articoli 21 - 24: Disposizioni finali**

DOVE TROVARE LE DISPOSIZIONI PIÙ IMPORTANTI DELLA DIRETTIVA SUL COMMERCIO ELETTRONICO?

- **Obiettivo principale**: mercato interno e libertà di fornire servizi della società dell'informazione (articolo 1).
- **Altri obiettivi** sono "la certezza del diritto e la fiducia dei consumatori" (considerando 7), assicurare un alto livello di protezione dei consumatori e la protezione dei minori (considerando 10)
- **Campo di applicazione**: senza pregiudizio per la protezione dei consumatori (articolo 1)
- **Definizioni** (articolo 2)
- **Informazioni di base** ai consumatori e agli altri destinatari (articoli 5, 6, 10)
- **Diritti quando si effettuano ordini online** (articolo 11)
- **Principi di responsabilità dell'intermediario** (articoli 12-15). I principi più importanti qui sono:
  - I fornitori di hosting non sono responsabili per i contenuti di terzi se, quando ne sono a conoscenza, rimuovono o disabilitano rapidamente l'accesso ai contenuti illegali (articolo 14)
  -

    - Divieto per gli Stati membri di imporre un obbligo generale di monitoraggio ai fornitori (articolo 15)
- **Codici di condotta** (articolo 16)
- **Risoluzione alternativa delle controversie** (articolo 17)
- **Azioni giudiziarie** "per porre fine ad ogni presunta infrazione e per prevenire ogni ulteriore deterioramento degli interessi coinvolti" (articolo 18)
- **Cooperazione tra Stati membri** (articolo 19)
- **Sanzioni** (articolo 20)

Dall'adozione della direttiva sul commercio elettronico nel 2000, i servizi digitali si sono evoluti, sollevando nuove sfide. Per esempio, il principio del “porto sicuro” sta dando ad alcune piattaforme uno spazio libero per non essere ritenute responsabili. Alcuni fornitori di servizi digitali non si assumono una responsabilità significativa o non danno ai consumatori un adeguato risarcimento se qualcosa va storto. Allo stesso modo, alcune iniziative volontarie hanno ritardato la tanto necessaria azione normativa. Alcune di queste questioni sono state affrontate nell'ambito del prossimo Digital Services Act.
Consumer PRO ha anche sviluppato altri due documenti sui temi del diritto generale dei consumatori e dei ricorsi collettivi che possono integrare questo capitolo in modo utile.

PROSPETTIVE: LA PROSSIMA LEGGE SUI SERVIZI DIGITALI

Il prossimo Digital Services Act (DSA) regolerà gli obblighi degli operatori e fornitori di servizi digitali che agiscono come intermediari nel loro ruolo di collegare i consumatori con beni, servizi e contenuti.
Mira a proteggere meglio i consumatori e i diritti fondamentali online, a stabilire un quadro efficiente di trasparenza e responsabilità per le piattaforme online e quindi a promuovere mercati digitali più equi e aperti.
A differenza della direttiva sul commercio elettronico, il DSA è un regolamento, quindi armonizzerà le regole in tutta l'UE e sarà direttamente applicabile. Le nuove regole dovrebbero garantire lo stesso livello di protezione a tutti i cittadini dell'UE.
Tra le altre cose, il DSA includerà :

- Misure per contrastare i contenuti illegali online, compresi beni e servizi, come un meccanismo per gli utenti che permetterà di segnalare tali contenuti, e per le piattaforme di cooperare con **"flaggers di fiducia";**
- Nuove regole sulla tracciabilità degli utenti commerciali nei marketplace online (noto anche come "know your business customer obligation"), volte a identificare meglio i venditori di merci illegali;
- Salvaguardie per gli utenti, compresa la possibilità di contestare le decisioni di moderazione dei contenuti delle piattaforme;
- Ulteriori misure di trasparenza per le piattaforme online, anche sugli algoritmi utilizzati per le raccomandazioni e sulla pubblicità mirata;
- Obblighi per le piattaforme online molto grandi di prevenire l'abuso dei loro sistemi, in particolare affrontando i rischi sistemici e includendo la supervisione attraverso audit indipendenti delle misure che adottano;

- Una nuova struttura di supervisione per affrontare la complessità dello spazio europeo digitale online in cui gli Stati membri avrebbero il ruolo principale, sostenuta da un nuovo consiglio europeo per i servizi digitali. Per le piattaforme online molto grandi, ci sarebbe un ruolo di supervisione e di applicazione rafforzato per la Commissione.

Mentre la DSA porterà molti miglioramenti necessari in termini di protezione dei consumatori nei servizi digitali, un punto in cui è improbabile che ci siano grandi cambiamenti è il regime di responsabilità per i marketplace online. La DSA manterrà molto probabilmente la responsabilità dell'intermediario principi di esenzione della direttiva sul commercio elettronico, anche se con alcuni chiarimenti e piccoli miglioramenti. Leggi e regolamenti a livello UE

REGOLAMENTO/ DIRETTIVA	DATA DI APPLICAZIONE	REVISIONE / VALUTAZIONE:TIPO DI MISURA	DATA SCADENZA	COMMENTO
		Rapporto d'esame CE (art. 21)	Prima del 17/07/2003, e in seguito ogni due anni	Nessuna valutazione formale ci è nota dal 2012. L'inchiesta settoriale della Commissione del 2017 può essere interessante dal punto di vista della concorrenza.
Direttiva sul commercio elettronico	17/01/2002(trasposizione)	Legge sui servizi digitali (DSA)	Proposta pubblicata nel dicembre 2020- Attualmente nella fase finale della procedura di co-decisione. L'adozione è prevista per il 2022	Proposta DSA presentata nel dicembre 2020 insieme al Digital Markets Act (DMA) che ha regole specifiche rivolte alle piattaforme gatekeeper.Argomenti chiave nel DSA dal punto di vista del consumatore: responsabilità degli intermediari, in particolare dei marketplace online; obblighi di conoscenza del cliente commerciale, procedure di notifica e azione, requisiti di trasparenza, applicazione e coordinamento tra gli Stati membri, obblighi in relazione alla pubblicità mirata e all'uso di sistemi di raccomandazione.
Piattaforma per la regolamentazione del business(P2BRegolamento)	12/07/2020	Linee guida CE sui requisiti di trasparenza delle classifiche (art. 5)	Pubblicato il 7 dicembre 2020Pubblicato il 7 dicembre 2020	
		La CE incoraggia i codici di condotta (art. 17)	Nessuna data	Un'analisi del loro funzionamento farà parte della revisione.
		Rapporto di revisione CE (art. 18)	13/01/2022 e ogni tre anni	
Direttiva Omnibus	28 novembre2021(trasposizione)28 maggio 2022(applicazione)	Articolo7-Trasposizione	Articolo 6 - Rapporto della Commissione e revisione.Rapporto da pubblicare da parte della CE entro il 28 maggio 2024, DQdi cibo e misure di vendita a domicilio.	

GIURISPRUDENZA

- **Re: Direttiva Omnibus**: non c'è ancora una giurisprudenza perché è divenuta applicabile solo a partire dal 28 maggio 2022.
- **Re: Direttiva eCommerce**: vedere la lista dei casi qui.

COSA POSSONO FARE I CONSUMATORI SE HANNO UN PROBLEMA?

- Tornare direttamente dal venditore/piattaforma (questo passo non è obbligatorio).
- Risoluzione alternativa delle controversie (ADR) possibile (questo passo non è obbligatorio).
- Autorità competenti degli Stati membri: varia da paese a paese e da argomento a argomento.

A livello nazionale
In Italia l'autorità preposta alla valutazione sull' applicazione e al controllo in materia di GDPR è il Garante della Privacy: https://www.garanteprivacy.it/

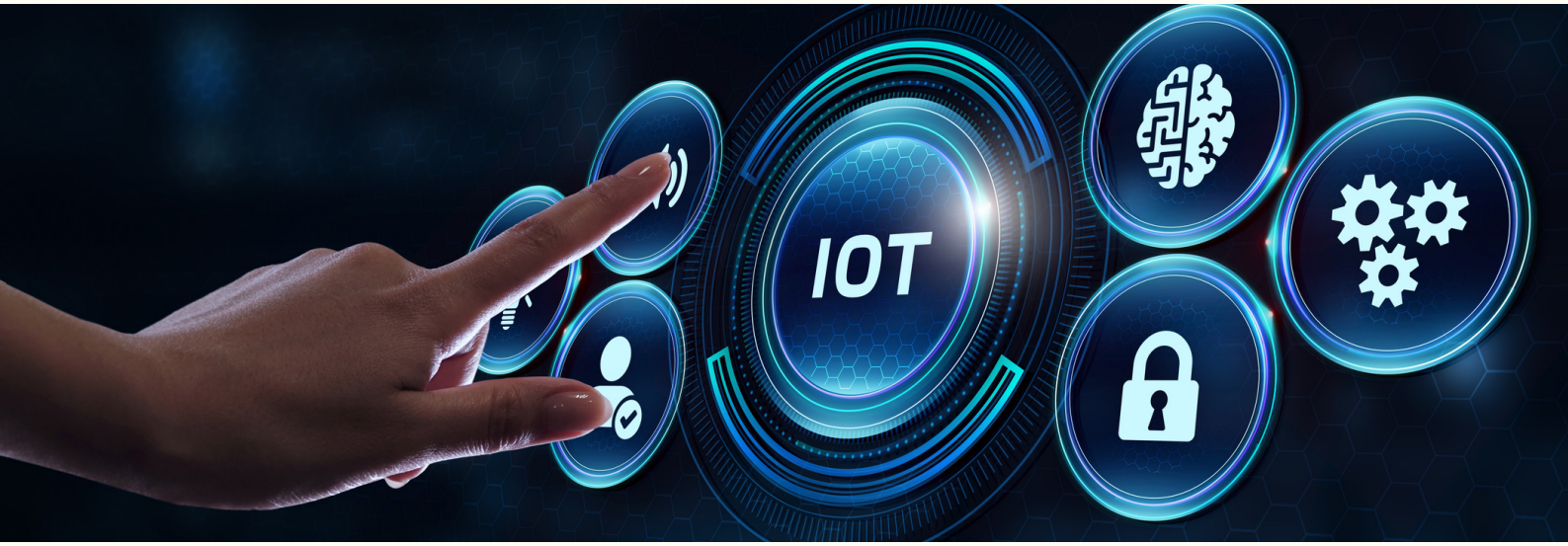
ULTERIORI RISORSE - SCHEDE, PUBBLICAZIONI, LINK

- Presentazione della Commissione europea sugli strumenti e gli obiettivi seguiti nella direttiva sul commercio elettronico (vedi qui)
- BEUC position paper Assicurare la protezione dei consumatori nell'economia delle piattaforme: (qui)
- BEUC documento di posizione Economia collaborativa (qui)
- Documento di posizione del BEUC su come far funzionare il Digital Services Act per i consumatori (qui)
- Documento di posizione del BEUC sulla proposta di legge sui servizi digitali (qui)
- Scheda informativa BEUC: La proposta di legge sui servizi digitali - proteggere meglio i consumatori (qui)
- Briefing del Parlamento europeo sulla proposta di legge sui servizi digitali (qui)
- Commissione europea - documento Q&A sulla legge sui servizi digitali (qui)

INTERNET DELLE COSE (IOT)

INTRODUZIONE E STORIA

Nell'arco degli ultimi anni, i dispositivi connessi sono diventati onnipresenti nella vita di molti consumatori. Mentre prima saremmo stati normalmente davanti a un computer per accedere a internet, ora portiamo sempre con noi smartphone connessi a internet ovunque andiamo. Allo stesso tempo, una quantità crescente di dispositivi quotidiani intorno a noi sono dotati di sensori e connessi a internet. Dalle caffettiere connesse alle telecamere di sicurezza, dalle automobili ai dispositivi medici, l'aumento dei dispositivi connessi è comunemente noto come "internet delle cose", o IoT.



PERCHÉ L'IOT È IMPORTANTE PER I CONSUMATORI

Negli ultimi anni, i dispositivi connessi sono diventati onnipresenti nella vita di molti consumatori, e l'aumento dei dispositivi connessi sta cambiando il modo in cui conduciamo le nostre vite. Mentre la digitalizzazione dei dispositivi fornisce molti benefici per i consumatori, i rischi e le sfide che porta sono altrettanto importanti, se non addirittura maggiori.

Per esempio, cosa succede quando il fornitore di servizi del vostro sistema di casa intelligente decide di chiudere i suoi server?
E chi è responsabile se la vostra smart TV è compromessa o non funzioni più a causa della mancanza di aggiornamenti del software?
E che dire dell'impatto sulla nostra privacy?

È quindi importante sviluppare politiche UE chiare e lungimiranti e un quadro giuridico che garantisca che i diritti dei consumatori siano garantiti in questo ambiente digitale interconnesso.

PRINCIPALI SFIDE ALL'INTERNO DELL'IOT

La connessione di una grande quantità di dispositivi a Internet solleva sia opportunità che rischi per i consumatori. Il mondo interconnesso promette un maggiore comfort, esperienze senza soluzione di continuità e miglioramenti potenzialmente significativi della qualità della vita. Le informazioni aggregate da questi dispositivi potrebbero anche portare a nuove intuizioni in aree come la scienza medica, l'intelligenza artificiale e la pianificazione urbana
.
Per esempio, una casa intelligente piena di dispositivi e sensori connessi può imparare le abitudini e le preferenze del suo proprietario, e adattare la sua funzionalità di conseguenza.

Allo stesso tempo, i diversi dispositivi individuali possono comunicare tra loro, in modo che per esempio un basso ritmo cardiaco rilevato da un orologio intelligente generi un messaggio urgente all'ospedale più vicino. Inoltre, la capacità di monitoraggio remoto dei dispositivi attraverso internet può aiutare gli individui che hanno bisogno di assistenza a mantenere la loro indipendenza, per esempio sbloccando le porte a distanza senza la necessità di camminare fino alla porta. In settori come industria e salute, l'internet delle cose è destinato ad avere effetti potenzialmente trasformativi sull'efficienza e l'accumulo di informazioni.
Ma le sfide che i dispositivi connessi portano sono molteplici dal punto di vista del consumatore. Toccano una vasta gamma di aree politiche e questioni: privacy e protezione dei dati, sicurezza informatica, obsolescenza dei prodotti, sostenibilità e consumo energetico, concorrenza, sicurezza, diritti dei consumatori, ecc.

Per esempio, i dispositivi connessi raccoglieranno tipicamente grandi quantità di dati sui loro utenti e sul loro ambiente. Questa raccolta diffusa di dati solleva una serie di preoccupazioni pressanti relative alla protezione dei dati e alla privacy. Poiché sempre più aspetti della nostra vita sono incorporati in una rete più ampia di sensori e dispositivi, crescono anche i rischi potenziali e la portata delle violazioni dei dati e degli attacchi informatici. Ogni nuovo dispositivo che colleghiamo a Internet aggiunge un'altra potenziale opprtunità di attacco, e la catena di dispositivi è spesso forte solo quanto il suo anello più debole. L'emergere e l'implementazione dell'intelligenza artificiale nelle tecnologie IoT pone anche sfide relative all'equità, alla responsabilità etc.

Altre sfide che emergono attraverso l'internet delle cose includono la limitazione artificiale dei cicli di vita dei prodotti, gli effetti lock-in e la responsabilità del prodotto.

Inoltre, i dispositivi in rete hanno un maggiore consumo di energia a causa dei componenti di rete richiesti. Gran parte di questo consumo energetico deriva dalla continua reattività dei dispositivi attraverso la rete (modalità idle). Friedli et al. (2016) hanno previsto che le perdite globali in standby aumenteranno da 7,5 TWh nel 2015 a 47 TWh nel 2025, sulla base del consumo in standby dei dispositivi in rete che sono permanentemente collegati alla rete elettrica.

I PRINCIPALI DIRITTI E OBBLIGHI DEI CONSUMATORI IN SINTESI

Quando si tratta di dispositivi connessi, si applicano anche i diritti dei consumatori applicabili ai dispositivi non connessi. Per esempio, le regole sulla garanzia legale (direttiva sui contenuti digitali, direttiva sulle vendite di beni) si applicano ai prodotti di consumo IoT. Si applicano anche le regole sull'informazione dei consumatori previste dalla direttiva sui diritti dei consumatori. In una certa misura , le regole della legislazione sulla sicurezza dei prodotti si applicano anche ai dispositivi IoT.

Tuttavia, a causa della connettività di questi dispositivi, si applicano obblighi specifici:

1) In primo luogo, i dispositivi che raccolgono dati personali sui consumatori devono essere sicuri di trattare questi dati secondo le regole stabilite nel GDPR. Queste regole includono, ma non si limitano, ai principi di minimizzazione dei dati, limitazione delle finalità e la protezione dei dati per progettazione, e l'obbligo di ottenere il consenso dell'utente a seconda delle finalità del trattamento dei dati.

2) In secondo luogo, secondo la direttiva sulle apparecchiature radio, a partire dal 2024, i produttori di dispositivi connessi dovranno garantire che i loro dispositivi mostrino un certo livello di sicurezza. Queste misure devono garantire che i dispositivi:

(i) non danneggino la rete causando un degrado inaccettabile del servizio;

(ii) incorporino garanzie per assicurare che i dati personali e la privacy dell'utente e dell'abbonato siano protetti

(iii) supportino certe caratteristiche che assicurino la protezione da frodi come il ransomware.

3) Secondo la direttiva sui contenuti digitali, i dispositivi connessi devono essere forniti con aggiornamenti, compresi quelli di sicurezza, per il periodo di tempo che i consumatori possono ragionevolmente aspettarsi. La durata di questo obbligo è legata al periodo di garanzia legale, ma può anche andare oltre.

A livello nazionale

In Italia il periodo di garanzia legale è di 2 anni dall'acquisto

4) In quarto luogo, secondo il Cybersecurity Act, quando esistono schemi di certificazione e si applicano al dispositivo connesso in questione, il produttore di tale dispositivo deve informare il consumatore sul periodo durante il quale il supporto di sicurezza sarà offerto agli utenti finali, in particolare per quanto riguarda la disponibilità di aggiornamenti relativi alla sicurezza informatica.

5) I consumatori dovrebbero avere consapevolezza che l'accesso ai servizi internet sia fornito in modo neutrale e non discriminatorio secondo il regolamento Open Internet. I fornitori di servizi internet devono trattare tutto il traffico internet allo stesso modo senza discriminazioni, restrizioni o interferenze ("neutralità della rete"). Mantenere l'accesso a internet aperto e neutrale è essenziale se vogliamo esercitare le nostre libertà fondamentali e i diritti democratici di partecipare alle odierne società online interconnesse. È anche una precondizione per beneficiare dell'Internet delle cose. I consumatori hanno bisogno di un internet illimitato e neutrale per usare i loro dispositivi connessi per accedere a notizie e contenuti culturali o per fare acquisti senza restrizioni.

6) Quando si tratta di regole sulla responsabilità del prodotto, la direttiva pertinente - la direttiva sulla responsabilità del prodotto - è stata redatta nel 1985, molto prima che si potesse considerare l'uso di dispositivi connessi, per non parlare di prevedere le sfide future. Non è più adatta ad affrontare le sfide dell'internet delle cose e a garantire un risarcimento ai consumatori quando le cose vanno male. Il processo di revisione di questa direttiva è in corso. In Aprile 2020, il BEUC ha fatto diverse raccomandazioni per garantire che le norme UE sulla responsabilità dei prodotti vengano aggiornate e adeguate per proteggere i consumatori nell'era digitale e all'IoT.

LEGGI E REGOLAMENTI A LIVELLO U

- Direttiva 2014/53/UE del Parlamento europeo e del Consiglio del 16 aprile 2014 concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE
- Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA (Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione e che abroga il regolamento (UE) n. 526/2013 (legge sulla cibersicurezza)
- Direttiva 2001/95/CE del Parlamento europeo e del Consiglio del 3 dicembre 2001 sulla sicurezza generale dei prodotti
- Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, su alcuni aspetti relativi ai contratti di fornitura di contenuti digitali e servizi digitali
- Regolamento Open Internet (Regolamento (UE) 2015/2120) del 25 novembre 2015.
- Regolamento (UE) 2015/2120 che stabilisce misure relative all'accesso aperto a Internet e modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica
- Rapporto della Commissione europea sull'inchiesta nel settore dell'Internet degli oggetti per i consumatori

* Altre leggi rilevanti, come il GDPR e l'acquis sui diritti dei consumatori non sono citati qui ma sono anche applicabili in un contesto IoT come qualsiasi altro prodotto o servizio. Ad esempio, se un dispositivo connesso elabora dati personali, dovrà essere conforme al GDPR.

GIURISPRUDENZA

Per quanto riguarda la "neutralità della rete" (vedi punto 5 del capitolo 3.4), la Corte di giustizia dell'UE, ha recentemente stabilito nelle cause C-854/19, C-5/20 e C-34/20 che le offerte che applicano una "tariffa zero"20 a specifiche app - e quindi le limitazioni che derivano dall'attivazione di queste opzioni (sulla larghezza di banda, sul tethering o sull'uso in roaming) - sono in violazione dell'articolo 3(3) del regolamento Open Internet e, quindi, sono illegali secondo il diritto UE. I fornitori di servizi dovrebbero quindi rivedere le loro pratiche commerciali in linea con questa interpretazione per garantire che rispettino pienamente le regole dell'UE sulla neutralità della rete. Un ragionamento simile potrebbe essere applicato dalla Corte ai fornitori di servizi che offrono una "tariffa zero" per le app associate ai dispositivi connessi (ad esempio, nel contesto di una campagna di marketing, un fornitore di servizi internet offre una tariffa vantaggiosa, cioè una tariffa zero, all'app utilizzata per controllare una telecamera intelligente).

COSA POSSONO FARE I CONSUMATORI SE HANNO UN PROBLEMA?

PDiverse leggi si applicano ai dispositivi connessi. A seconda della legge applicabile, i consumatori avranno diverse opzioni.

- Se si tratta di un problema relativo ai loro dati personali (vedi punto 1) nel capitolo 3.4), si applica il GDPR.21
- Secondo la direttiva sulle apparecchiature radio, se c'è un problema con la sicurezza dei loro dispositivi (vedi punto 2 nel capitolo 3.4), a partire dal 2024, i consumatori potranno notificare le loro autorità nazionali di sorveglianza del mercato (spesso l'autorità delle telecomunicazioni), che inizieranno un'indagine su quel dispositivo specifico. La decisione dell'autorità di sorveglianza del mercato può anche arrivare a ordinare il ritiro di quel prodotto dal mercato.

- Se il dispositivo non è stato fornito in conformità con le aspettative dei consumatori per quanto riguarda la fornitura di aggiornamenti di sicurezza (vedi punto 3 del capitolo 3.4), i consumatori hanno il diritto di rescindere il contratto, ricevere una riduzione proporzionata del prezzo o richiedere che il dispositivo sia reso conforme (vedi direttiva sui contenuti digitali).

- Secondo il Cybersecurity Act, se la fornitura di aggiornamenti di sicurezza è più breve di quanto annunciato dal produttore (vedi punto 4 del capitolo 3.4), i consumatori possono presentare un reclamo a un organismo nazionale. Se i consumatori non sono soddisfatti della decisione presa dall'organismo nazionale, hanno diritto a un ricorso giudiziario efficace.

- Se la neutralità della rete non è rispettata (vedi punto 5 del capitolo 3.4), i consumatori possono presentare un reclamo all'autorità di regolamentazione delle loro telecomunicazioni, che dovrà agire di conseguenza.

ULTERIORI RISORSE - SCHEDE, PUBBLICAZIONI, LINK

Documento di lavoro dei servizi della Commissione europea - Far progredire l'Internet degli oggetti in Europa Indagine settoriale della Commissione europea sull'Internet degli oggetti per i consumatori (IoT)
Documento di posizione del BEUC: Proteggere i consumatori europei nel mondo dei dispositivi connessi BEUC factsheet: Garantire la sicurezza informatica dei prodotti di consumo
AK EUROPA - Le aspettative dei consumatori sull'Internet delle cose

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110
https://ec.europa.eu/commission/presscorner/detail/en/ip_22_402
https://www.beuc.eu/publications/beuc-x-2021-091_protecting_european_consumers_in_the_world_of_connected_devices.pdf
https://www.beuc.eu/publications/beuc-x-2020-126_ensuring_cybersecure_consumer_products.pdf
https://www.akeuropa.eu/sites/default/files/2021-02/Consumers expectations of the Internet of Things_0.pdf

CONSUMERPRO
BOOSTING PROFESSIONALS IN CONSUMER PROTECTION

European Commission