Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

a. a. 2022/2023

Il pagamento mediante dati personali

Relatore: Prof.ssa Giovanna Marchetti

Studente: Martina Zefi

Matricola 2015342

INDICE

INTRODUZIONE

Nell'era digitale in cui siamo immersi, l'uso dei dati personali ha assunto un ruolo centrale nella nostra vita quotidiana, influenzando molteplici aspetti, tra cui le decisioni d'acquisto, la personalizzazione dei servizi online e la profilazione degli utenti. Parallelamente a questa crescente rilevanza dei dati personali, si è sviluppata una nuova forma di transazione economica: il pagamento mediante dati personali. Questo concetto suscita una serie di interrogativi complessi e interdisciplinari che toccano aspetti etici, giuridici ed economici.

La questione cruciale riguarda il processo di estrazione, ovvero come vengono raccolti e da dove provengono questi dati. Normalmente i dati possono essere ottenuti direttamente dalla persona interessata o da terze parti che già li possiedono, ma a seguito dell'avanzamento, sempre più pervasivo e invasivo, delle tecnologie digitali, la raccolta dei dati è ora più semplice che mai: grazie all'uso diffuso di dispositivi che tracciano le azioni degli utenti, le persone lasciano tracce di dati dietro di sé, spesso senza rendersene conto. Questi dati vengono poi raccolti da chi gestisce tali dispositivi e da coloro che ne hanno accesso.

Ci sono due strategie principali per raccogliere dati: la prima è quella di incentivare l'utilizzo di beni e servizi che, grazie alla tecnologia adottata, registrano automaticamente informazioni sugli utenti durante il loro utilizzo; la seconda, invece, consiste nel raccogliere informazioni direttamente dalle persone interessate. Le tipologie di dati raccolti sono diverse nei due casi: nel primo, le informazioni sono filtrate attraverso l'interazione dell'utente con il servizio, mentre nel secondo caso, le informazioni riguardano principalmente i comportamenti delle persone[1].

In entrambi i casi, è richiesta una forma di collaborazione: se nel primo caso l'interessato deve fornire consapevolmente le informazioni, nel secondo caso la collaborazione è passiva, poiché l'atto di utilizzare un bene o servizio genera automaticamente dati suscettibili di registrazione.

Tuttavia, è importante notare che la raccolta di dati non è libera, almeno nella nostra giurisdizione. Le leggi sulla protezione dei dati personali stabiliscono condizioni legali per il trattamento dei dati, tra cui il consenso dell'interessato. Questo consenso, spesso, è diventato

[1] S. Thobani, *Il pagamento mediante dati personali*, *Annuario 2021 Osservatorio Giuridico sulla Innovazione Digitale*, a cura di S. Orlando e G. Capaldo, Sapienza Università Editrice, 2021, p. 361

una condizione fondamentale e viene frequentemente richiesto come parte integrante dell'offerta di beni e servizi.

Questa pratica, chiamata "tying," collega l'uso dei servizi alla prestazione del consenso al trattamento dei dati, garantendo così la legittimità della raccolta e del trattamento dei dati.

Esistono diverse modalità in cui avviene questa "offerta" di beni e servizi in cambio dei dati personali. Ad esempio, nel mondo online, il modello di business si basa sulla fornitura gratuita di servizi, ma richiede agli utenti di acconsentire al trattamento dei dati per poterne usufruire. In altri casi, il consenso al trattamento dei dati è richiesto non per l'accesso al servizio stesso, ma per ottenere sconti o vantaggi speciali. In alcuni rari casi, viene offerta una compensazione diretta in denaro a coloro che acconsentono al trattamento dei propri dati.

Tutte queste situazioni implicano l'uso dei dati come strumento di accesso a una sorta di controprestazione, che può essere un servizio, uno sconto o anche una somma di denaro. È stato pertanto coniato il termine "pagamento" mediante dati personali, sottolineando come questi dati, in modo simile al denaro, rappresentino una forma di valore.[2]

Dal punto di vista legale, queste pratiche sollevano due quesiti principali. Prima di tutto, c'è la questione della loro liceità: è lecito "pagare" con dati personali? È giuridicamente valido subordinare l'accesso a beni o servizi al consenso al trattamento dei dati personali? In secondo luogo, una volta stabilita la liceità di tali operazioni, sorge la questione di come esse siano regolate dal punto di vista normativo[3] e, in particolare, in che modo i consumatori vengano tutelati.

[2] *Ivi*, p. 362

[3] *Ivi*, p. 363

CAPITOLO I

LE OPERAZIONI TYING

1. Modelli di business

Possiamo individuare due modelli di business che si caratterizzano per il fatto che il consumatore non paghi un prezzo in denaro, ma presti, invece, il consenso al trattamento dei propri dati personali.

Il primo modello a cui ci riferiamo è il modello zero-price, che prevede l'erogazione di servizi senza che l'utente debba eseguire una controprestazione pecuniaria, il quale, invece, acconsente al trattamento dei propri dati personali per diverse finalità, necessarie per eseguire una prestazione richiesta oppure per il perseguimento di interessi commerciali che sono estranei al rapporto contrattuale posto in essere tra l'utente e professionista che eroga il servizio.

Ci si pone un interrogativo: è veramente a prezzo zero? Il valore economico dei dati personali forniti dall'utente deriva dal trattamento di aggregazione, profilazione, analisi svolta dall'impresa sull'enorme numero di dati accumulati.

Ci troviamo, quindi, davanti ad un modello di business per la fornitura di servizi digitali che, in teoria è a prezzo zero, ma in realtà nasconde al suo interno un valore economico, cioè quello dei dati, i quali vengono ceduti all'impresa: si parla non del singolo dato in quanto tale, ma è proprio il trattamento di questo enorme numero di dati che genera un valore economico per l'impresa, anche perchè l'impresa può cedere questi dati a terzi.

Queste operazioni vengono chiamate e sono conosciute come operazioni di tying.

Anche se il servizio sembra "gratuito", la vera merce è rappresentata dall'utente, perchè i dati vengono a conseguire l'asset da cui l'impresa trae profitto.

Sul tema ci sono numerose discussioni, in particolare sulla legittimità di queste operazioni: si discute se effettivamente il diritto alla protezione e poi al trattamento dei dati personali sia un diritto disponibile oppure no, poiché è possibile cedere il proprio diritto alla protezione dei dati personali, consentire al trattamento dei dati personali e quindi usarli come merce di scambio[4].

[4] C. Irti, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, spec. 45 ss

A lungo la risposta è stata di tipo negativo perchè questo diritto era considerato un diritto indispensabile e quindi era impossibile darne una valorizzazione economica[5]; ma, in seguito, a fronte della diffusione della prassi rispetto a questo fenomeno, quest'idea è stata via via abbandonata. Queste operazioni si sono legittimate, tanto più che si è cominciato a dire che l'utente non sta trasferendo la proprietà dei propri dati personali, ma sta semplicemente consentendo di utilizzarli prestando il suo consenso (eventualmente può anche revocarlo).

La Cassazione, infatti, pur ritenendo leciti, in via di principio, i contratti di scambio tra servizi digitali e dati personali, li ha ritenuti ammissibili solo a condizione che, da un lato, il consenso non sia viziato da possibili disorientamenti o slealtà comunque adottate dal titolare del trattamento, e, dall'altro, che la prestazione del professionista non sia infungibile e irrinunciabile per l'interessato.

Il secondo modello di business è il modello personal data economy: il consumatore acconsente al trattamento dei dati personali per finalità diverse rispetto a quelle dell'erogazione del servizio, ma in questo caso la piattaforma attribuisce un vero e proprio valore ai dati personali, tant'è che riconosce agli utenti in tutto e in parte il valore che essa stessa attribuisce ai dati personali, attribuendoli una somma di denaro (monetizzazione del dato).[6]

1.1. Liceità

Una delle questioni più dibattute nel contesto della protezione dei dati personali riguarda l'ammissibilità delle operazioni in cui i dati personali vengono scambiati in cambio di una controprestazione, sollevando dubbi sulla liceità della subordinazione del consenso al trattamento dei dati personali per l'accesso a beni o servizi. Questo argomento è al centro di una complessa e articolata discussione legislativa e giuridica che richiede un'analisi dettagliata[7].

Dal punto di vista normativo, il Regolamento generale sulla protezione dei dati (GDPR) fornisce alcune linee guida chiare, ma non risponde in modo definitivo a questa questione complessa.

---

[5] F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018.

[6] E. Battelli, *I modelli negoziali di business degli operatori digitali a "prezzo zero" non sono gratuiti*, Altalex, 2022.

[7] S. Thobani, *Il pagamento mediante dati personali* cit., p. 363

L'articolo 7, paragrafo 4, del GDPR affronta il tema del consenso al trattamento dei dati personali in relazione all'accesso a beni o servizi. Questa disposizione stabilisce che il consenso al trattamento dei dati personali non è considerato liberamente prestato se l'accesso a un bene o servizio è subordinato al consenso stesso, a meno che il trattamento dei dati non sia strettamente necessario per l'esecuzione di un contratto. In altre parole, se il trattamento dei dati è indispensabile per fornire il bene o servizio richiesto, non ci sono dubbi sulla sua liceità. Tuttavia, se il trattamento dei dati non è strettamente necessario per l'adempimento del contratto, la questione cruciale diventa la libertà del consenso al trattamento.

Il GDPR non vieta esplicitamente le operazioni di "tying"[8], ma enfatizza la necessità che il consenso sia liberamente prestato. Qui sorge la principale sfida interpretativa: il consenso è davvero libero se è subordinato all'accesso a un bene o servizio? Se il consenso non è considerato libero, il trattamento dei dati che ne deriva potrebbe essere illecito, in quanto la libertà del consenso è un prerequisito fondamentale per la liceità del trattamento dei dati[9]. Ciò potrebbe comportare un divieto delle operazioni di "tying." Tuttavia, se il consenso è considerato libero, la situazione cambia.

Il GDPR non fornisce una risposta definitiva a questa domanda, il che riflette una scelta deliberata del legislatore europeo. Una versione precedente del GDPR aveva stabilito un divieto esplicito delle operazioni di "tying," ma questa disposizione è stata attenuata nella versione finale del regolamento dopo una valutazione attenta degli interessi in gioco[10].

Questa incertezza normativa ha portato a divergenze di opinione tra gli interpreti: alcuni sostengono fermamente che richiedere il consenso come condizione per l'accesso a beni o servizi non sia ammissibile, poiché il consenso non può essere considerato libero in queste circostanze. Questa è l'opinione dell'autorità garante[11] per la protezione dei dati personali[12] e di altre autorità garanti nazionali europee.

---

[8] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Draft Report 17 December 2012*, 2012/0011(COD), amendment no 107.

[9] Cfr. S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità, Europa e diritto privato 2/16*, Giuffrè Editore, 2016, pp. 513- 517.

[10] S. Thobani, *Il pagamento mediante dati personali* cit., pp. 364, 365

[11] Cfr. S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità* cit., pp. 530 – 540.

[12] *Linee Guida in materia di attività promozionale e contrasto allo spam*, in Registro dei provvedimenti 4 luglio 2013, n. 330.

D'altro canto, ci sono interpretazioni che sostengono che le operazioni di "tying" possono essere legittime, purché siano offerte alternative equivalenti per gli utenti. In tal caso, gli utenti avrebbero una vera scelta nel concedere o meno il consenso al trattamento, poiché avrebbero accesso al bene o servizio anche senza prestare il consenso[13].

Inoltre, esistono indicazioni contrastanti nei corpi normativi europei. Mentre le norme sulla protezione dei dati personali guardano con sospetto alle operazioni di "tying," le norme a tutela dei consumatori si limitano a prevedere rimedi per i consumatori che "pagano" con dati personali, senza mettere in discussione la liceità di tali operazioni.

In conclusione, la liceità del "pagamento" mediante dati personali è un tema complesso e controverso che coinvolge considerazioni legislative, giuridiche ed etiche. Mentre ci sono diverse interpretazioni legislative e giuridiche, la tendenza generale sembra essere quella di un divieto o di una severa limitazione delle operazioni di "tying" per garantire la libertà del consenso dei consumatori. Tuttavia, questa è una questione ancora aperta e soggetta a evoluzione normativa e giurisprudenziale, poiché le sfide legate all'equilibrio tra la protezione dei dati personali e la fornitura di beni e servizi digitali continuano a evolversi.[14]

1.2 Trasparenza

La questione dello scambio tra dati personali e servizi riveste un ruolo cruciale sia nella normativa sulla protezione dei dati personali che nella legislazione a tutela dei consumatori. Questo scambio richiede, in primo luogo, un elevato grado di trasparenza, che emerge chiaramente dalle disposizioni normative.

In merito alla protezione dei dati personali, il Regolamento Generale sulla Protezione dei Dati (GDPR) stabilisce requisiti specifici per il consenso al trattamento dei dati personali.[15] Questi requisiti pongono l'accento sulla necessità che il consenso sia informato e specifico. Ciò significa che il soggetto interessato deve essere debitamente informato delle finalità del trattamento prima di esprimere il consenso, e il consenso stesso deve riguardare specifiche

[13] Comitato europeo per la protezione dei dati personali, *Guidelines 5/2020*, par. 37.

[14] S. Thobani, *Il pagamento mediante dati personali* cit., p. 369.

[15] Art. 4, numero 11 GDPR: "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento"*

finalità di trattamento. In altre parole, il consenso deve coprire solo i trattamenti di dati per i quali l'interessato è stato informato in modo chiaro e dettagliato.

Sia nel caso in cui i dati personali siano raccolti direttamente dall'interessato che, quando vengono acquisiti da terze parti, l'interessato deve essere informato in merito ai dati trattati, alle finalità del trattamento, ai soggetti che possono accedere ai dati e all'esistenza di processi decisionali automatizzati (articoli 13 e 14). Il consenso deve essere riferito a questo trattamento specificamente delineato e deve essere concesso "per una o più specifiche finalità" (articolo 6, paragrafo 1, lettera a)[16]. Inoltre, l'interessato deve essere informato sulla base giuridica del trattamento, ovvero se il consenso è la base giuridica o se vi è un'altra base legittima per il trattamento.

Questo significa che, se il consenso al trattamento è richiesto come condizione per accedere a un bene o servizio, l'interessato deve essere reso consapevole che la richiesta di dati è una scelta del titolare dei dati e non un obbligo legale. Inoltre, deve essere chiaro che in caso di mancato consenso, l'interessato non potrà accedere al bene o servizio. Questa trasparenza è particolarmente importante quando si praticano operazioni di tying (vincolo di condizionare l'accesso a un servizio al consenso al trattamento dei dati).

È interessante notare che la normativa a tutela dei consumatori affronta anche questa questione, dimostrando l'interconnessione tra i due corpus normativi. In alcune giurisdizioni, le autorità preposte alla concorrenza e al mercato hanno sanzionato la pubblicità ingannevole di offerte che presentavano servizi come gratuiti[17], ma richiedevano il consenso al trattamento dei dati personali anziché un pagamento in denaro. Queste autorità hanno sottolineato l'importanza di considerare il consenso al trattamento dei dati come una "prestazione passiva"[18] e il dato personale come un possibile oggetto di scambio economico.[19]

La Commissione Europea ha anche sottolineato che la violazione della normativa sulla protezione dei dati può essere rilevante per valutare la trasparenza di una pratica commerciale, soprattutto considerando il "valore economico de facto" dei dati personali. Quindi, la mancanza

[16] *Ivi*, p. 370

[17] AGCM, provv. Facebook – condivisione dati con terzi, 29 novembre 2018, n. 27432.

[18] AGCM, provv. 20 dicembre 2001, n. 10276, cit.

[19] S. Thobani, *Il pagamento mediante dati personali* cit., p. 372

di comunicazione chiara ai consumatori sull'uso commerciale dei dati personali può essere considerata un'omissione ingannevole di informazioni rilevanti[20].

In conclusione, la trasparenza è un elemento chiave nelle operazioni in cui i dati personali sono scambiati con beni o servizi. La normativa sulla protezione dei dati personali e la legislazione a tutela dei consumatori convergono nell'esigere questa trasparenza, sia per proteggere l'interessato che per garantire il consumatore.[21]

1.3 Nesso di corrispettività

Un altro aspetto da considerare è il nesso di corrispettività tra il consenso per il trattamento dei dati e il bene o servizio la cui fruizione è subordinata a questo consenso. Come viene definito questo nesso e quali implicazioni comporta per la relazione tra interessato/utente e il fornitore del servizio?

Iniziamo esaminando le implicazioni per il consumatore. Il riconoscimento di un nesso di corrispettività, almeno in termini pratici, tra il consenso al trattamento dei dati e l'accesso a beni o servizi ha portato prima gli studiosi e successivamente il legislatore a riconoscere rimedi a favore dei consumatori quando si tratta di accordare il proprio consenso in cambio di un servizio.[22]

In questa direzione, la direttiva 2019/770 sui contratti di fornitura di contenuto e servizi digitali, insieme alla direttiva 2019/2161 per la protezione dei consumatori, ha ampliato le tutele a beneficio dei consumatori, sia che essi paghino un corrispettivo in denaro, sia che "paghino" in dati.

In merito al nesso di corrispettività tra dati e servizi, vale la pena notare due aspetti. Innanzitutto, la direttiva 770/2019 non richiede più che il consumatore fornisca attivamente i dati per applicare le tutele.[23] In altre parole, il nesso di corrispettività è considerato sussistente ogni volta che il consenso dell'individuo è necessario per il trattamento dei dati, indipendentemente dal fatto che l'utente abbia fornito attivamente le informazioni o sia stato

[20] Commissione europea, *Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali*, 25 maggio 2016, 28.

[21] S. Thobani, *Il pagamento mediante dati personali* cit., p. 373.

[22] *Ibidem*

[23] *Ivi*, p. 374

coinvolto in modo passivo (ad esempio, attraverso il monitoraggio del comportamento online).[24]

In secondo luogo, è importante notare che i rimedi disponibili per i consumatori possono variare in base al tipo di corrispettivo fornito. Ad esempio, in caso di difetto di conformità del contenuto o del servizio digitale, la riduzione del prezzo è prevista solo quando è stato effettuato un pagamento in denaro. Questo potrebbe sembrare ovvio poiché solo in caso di pagamento in denaro è possibile restituire una somma di denaro. Tuttavia, questo non tiene conto completamente del valore dei dati personali, che non sono equiparabili al denaro.

Questi sono gli aspetti legati ai consumatori, ma cosa accade dal lato del fornitore di servizi? Prima di tutto, potrebbe sorgere la domanda se il nesso di corrispettività comporti obblighi per l'individuo che acconsente al trattamento dei dati per accedere a un servizio. Ad esempio, potrebbe essere necessario stabilire se il fornitore abbia diritto a ricorrere a rimedi (e quali) nel caso in cui l'individuo fornisca informazioni false.[25]

È importante poi esaminare cosa succede al servizio fornito se l'individuo revoca il consenso al trattamento dei dati. In questo caso, il servizio può essere interrotto? Il Regolamento europeo sulla protezione dei dati stabilisce il diritto di revocare il proprio consenso in qualsiasi momento, sottolineando che il consenso non è libero se l'individuo non può revocarlo senza subire conseguenze negative.

Tuttavia, se si ritiene che le operazioni di tying siano illegali, allora la revoca[26] del consenso non dovrebbe in alcun modo influire sul servizio. Questo rappresenterebbe un singolare nesso di corrispettività, in quanto non vi è alcun legame tra le due parti e l'interruzione del servizio costituirebbe un impedimento indebito alla libertà dell'individuo. Solo se si considera che le operazioni di tying siano legali, il servizio potrebbe essere interrotto in seguito alla revoca del consenso, poiché in questo caso il nesso di corrispettività è ritenuto valido e il suo funzionamento è bilaterale.[27]

---

[24] *Ivi*, p. 375

[25] *Ivi*, p. 376

[26] Cfr. S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità* cit., pp. 553 ss.

[27] S. Thobani, *Il pagamento mediante dati personali* cit., p 377.

CAPITOLO II

LA DISCIPLINA DEL MERCATO DI DATI PERSONALI

2. La diffusione di nuovi prodotti in forma di contenuti e servizi digitali

La digitalizzazione e l'avvento di Internet hanno portato alla nascita e alla diffusione di nuovi prodotti in forma di contenuti e servizi digitali, determinando un incremento degli scambi internazionali, fenomeno che dal 2014 ha portato la Commissione Europea ad introdurre tra le sue priorità la creazione del Digital Single Market, adottando una pluralità di iniziative destinate a promuovere la digitalizzazione e a rispondere alle nuove sfide che essa solleva per gli operatori del diritto. La Commissione, difatti, avendo realizzato l'importanza delle tecnologie digitali e di Internet, ha deciso di impegnarsi per innovare il mercato unico europeo, in quanto, fino a quel momento sia le aziende che i consumatori si trovavano di fronte a barriere nell'utilizzo di strumenti e servizi online, che impedivano non solo ai cittadini, ma anche ai governi, di poter beneficare appieno della digitalizzazione. L'obiettivo posto dalla Commissione è, quindi, creare un Mercato Unico Digitale in cui sia garantita la libera circolazione di merci, persone, servizi, capitali e dati, e in cui cittadini e le imprese possano accedere in modo trasparente ed equo a beni e servizi online, indipendentemente dalla loro nazionalità e da dove risiedano.

La Commissione Europea ha delineato una serie di obiettivi chiave per promuovere lo sviluppo digitale nell'Unione Europea. Questi obiettivi includono:

1. Promuovere l'e-commerce: eliminare il geoblocking e migliorare l'efficienza delle consegne transfrontaliere;
2. Modernizzare le norme sul copyright per adattarle all'era digitale;
3. Aggiornare le norme audiovisive: lavorare con le piattaforme digitali per promuovere film europei, proteggere i bambini dai contenuti dannosi e affrontare l'incitamento all'odio online, creando così un ambiente digitale più sicuro ed equo.
4. Rafforzare la sicurezza informatica: aumentare la capacità dell'Unione Europea di rispondere agli attacchi informatici rafforzando l'Agenzia europea per la sicurezza informatica (ENISA) e migliorando la cybersecurity in tutta l'UE.

5. Promuovere l'economia dei dati europea: creare norme per il libero flusso di dati non personali tra gli Stati Membri, sfruttando così il potenziale della European Data Economy.
6. Garantire la connettività Internet: assicurare a tutti i cittadini europei un accesso adeguato a Internet per favorire la partecipazione all'economia digitale e promuovere la "connectivity for a European gigabit society";
7. Adattare le regole ePrivacy all'ambiente digitale in evoluzione;
8. Sostenere l'adozione delle nuove tecnologie: Aiutare grandi e piccole imprese, ricercatori, cittadini e autorità pubbliche a sfruttare al massimo le nuove tecnologie, garantendo che tutti abbiano le competenze digitali necessarie e finanziando la ricerca dell'UE in settori come la salute digitale e il calcolo ad alte prestazioni.

Questi obiettivi riflettono l'impegno dell'Unione Europea nell'adattarsi e nel prosperare nell'era digitale, garantendo al contempo un ambiente equo, sicuro e accessibile per tutti i cittadini e le imprese europee.

La Commissione Europea ha strutturato, perciò, la sua strategia su tre pilastri fondamentali:

1. Migliorare l'accesso ai beni e ai servizi digitali: l'obiettivo è garantire un accesso più facile e aperto sia per i consumatori che per le aziende ai beni e servizi online europei. Ciò comporta la rimozione delle barriere all'e-commerce, rendendo possibile per le persone fare acquisti online in modo semplice e senza restrizioni transfrontaliere. Questo pilastro mira a creare un ambiente in cui i consumatori possano accedere a una vasta gamma di prodotti e servizi digitali da qualsiasi parte dell'Unione Europea.
2. Creare un ambiente favorevole per i network e i servizi digitali: questo pilastro si concentra sulla creazione di un ambiente in cui le infrastrutture digitali, comprese le reti e i servizi, possano prosperare. Questo è reso possibile attraverso infrastrutture veloci, sicure e affidabili. Elementi chiave di questa componente includono la cybersecurity, la protezione dei dati e la trasparenza delle piattaforme online. Assicurare la sicurezza e la protezione delle informazioni digitali è cruciale per creare fiducia tra i consumatori e promuovere la crescita degli affari online.
3. Utilizzare il digitale come motore per la crescita economica: Questo pilastro sottolinea il ruolo del digitale come catalizzatore per la crescita economica. L'obiettivo è massimizzare i benefici derivanti dalle tecnologie digitali per ogni cittadino europeo. Ciò implica l'adozione diffusa delle tecnologie digitali in vari settori economici, garantendo che le

persone abbiano accesso alle competenze digitali necessarie per partecipare all'economia digitale e sostenendo l'innovazione e la ricerca nel campo delle tecnologie digitali.

Questi tre pilastri costituiscono la base della strategia del Digital Single Market, unendo gli sforzi per rimuovere le barriere, garantire la sicurezza e sfruttare appieno il potenziale economico del mondo digitale all'interno dell'Unione Europea.[28]

Naturalmente, le regole tradizionali non si apprestano a regolare adeguatamente i nuovi fenomeni e a tutelare gli attori dello scenario attuale, in particolare dei consumatori.
A tal proposito, tra le sfide più impattanti della *digital age* figurano quelle sollevate dalla diffusione dei contratti di fornitura di contenuto digitale, ovvero contratti funzionali all'accesso e alla fruizione di beni e servizi in formato digitale. Sfide che hanno portato all'adozione della direttiva UE 2019/770[29] che attraverso i suoi principali obiettivi mira a:

- Garantire ai consumatori un migliore accesso ai contenuti e servizi digitali, anche sotto il profilo della tutela
- Semplificare la fornitura di contenuti e servizi digitali da parte delle imprese, a fronte delle difficoltà che sarebbero sorte a causa della difforme regolamentazione del fenomeno da parte dei singoli Stati membri

In riferimento al secondo punto, al fine di adeguare la normativa italiana alla direttiva UE 2019/770, il Consiglio dei ministri ha approvato in via definitiva il d.lgs. n. 206/2005 che introduce nel codice del consumo gli artt. 135 *octies* ss. volti a disciplinare determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali conclusi tra consumatore ("persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta") e professionista ("la persona fisica o giuridica che agisce nell'esercizio della propria attività imprenditoriale, commerciale, artigianale o professionale, ovvero un suo intermediario"): la conformità del bene al contratto, i rimedi in caso di difetto di conformità o di mancata fornitura, la modifica del contenuto o del servizio digitale, la consegna e i rimedi per la consegna tardiva. Suddette modifiche al codice

[28] L. Berto, *Il Digital Single Market: di cosa tratta e che punto siamo*, Ius in itinere, 2018.

[29] G. Marchetti, S. Thobani, *La tutela contrattuale dei consumatori di contenuti e servizi digitali, Manuale di diritto privato delle nuove tecnologie*, a cura di G. Magri, S. Martinelli e S. Thobani, Giappichelli, 2022, p. 36.

del consumo acquistano efficacia a decorrere dal 1° gennaio 2022 e si applicano alle forniture di contenuto o servizi digitali che avvengono a partire da questa data, anche se il contratto è stato concluso in una data precedente.

Il quadro normativo di riferimento europeo non si esaurisce nella direttiva UE 2019/770 ma, al contrario, si tratta di una disciplina complessa e composita che si basa su diverse fonti normative, tra cui:

- La direttiva UE 2011/83 sui diritti dei consumatori, in particolare riguarda informazioni generali, diritto di recesso, pagamento, contratti a distanza, fuori locali commerciali e dovere informativi
- La direttiva UE 2019/2161 che modifica la direttiva 93/13/CEE del Consiglio
- La direttiva OMNIBUS che mira ad una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori
- Il regolamento UE 2016/679 sulla protezione dei dati personali (GDPR)[30]

2.1 I modelli contrattuali di fornitura di contenuto digitale e servizi digitali

La direttiva 770/2019 lascia ampia libertà agli Stati membri di regolare la natura giuridica dei contratti per la fornitura di contenuto o servizi digitali, ovvero quei contratti con cui il professionista fornisce o si obbliga a fornire un contenuto digitale o un servizio digitale al consumatore che corrisponde un prezzo oppure si obbliga a corrispondere un prezzo[31].

Ai fini dell'applicazione della disciplina prevista a tutela del consumatore non è necessario che il contratto appartenga a uno specifico tipo, anche la direttiva 770 risulta generica riferendosi a "qualsiasi contratto" con cui vengono forniti il contenuto o i servizi digitali e utilizzando, nell'art. 3 della stessa, il termine trader (operatore economico), privo di valenza giuridica specifica.

D'altra parte, invece, vengono definiti in modo estremamente chiaro i concetti di "contenuto digitale" e "servizio digitale". L'art. 1 della direttiva 770/2019 definisce un

[30] *Ivi*, p. *37*

[31] Art. 3, par. 1 della Proposta di direttiva relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 9 dicembre 2015, COM (2015) 634.

contenuto digitale come l'insieme di "dati prodotti e fornito in formato digitale"[32], mentre l'art. 2 n.2 della medesima direttiva definisce un servizio digitale come " *un servizio che consente al consumatore di creare, trasformare, archiviare i dati o di accedervi in formato digitale*" oppure "*un servizio che consente la condivisione di dati in formato digitale caricati o creati dal consumatore e da altri utenti di tale servizio o qualsiasi altra interazione con tali dati*".

Suddetta disciplina si applica indipendentemente dal supporto utilizzato per la trasmissione del contenuto o servizio digitale (materiale, streaming, ecc.) o per darvi accesso[33] e, in particolare, sono due i modelli contrattuali a cui si riferisce. Il primo è quello del contratto oneroso a prestazioni corrispettive nel quale il professionista fornisce o si obbliga a fornire un contenuto o un servizio digitale e il consumatore paga o si obbliga a pagare un prezzo, che può consistere in una somma di denaro, oppure in una rappresentazione digitale del valore dovuto.

Il secondo modello prevede che il consumatore autorizzi il professionista al trattamento per scopi commerciali dei suoi dati personali, fenomeno che apre il complesso tema della patrimonializzazione e commerciabilità dei medesimi.

L'orientamento interpretativo che rifiuta la possibilità di considerare i dati personali come una controprestazione si basa su alcune fondamentali considerazioni. In primo luogo, i dati personali sono di natura peculiare e la loro protezione è un diritto fondamentale, pertanto non dovrebbero essere trattati come una merce commerciabile. Inoltre, si cerca di evitare che il consumatore dia il proprio consenso al trattamento dei dati personali in modo ingannevole, credendo che l'operazione sia gratuita, anche se in realtà i dati personali vengono scambiati come parte di un accordo implicito.

Il legislatore europeo ha affrontato questa questione e inizialmente aveva introdotto il concetto di controprestazione in relazione ai dati personali nel progetto della direttiva 770/2019. Tuttavia, nella versione definitiva della direttiva, tale riferimento è stato rimosso, ma nonostante questo, la direttiva 770/2019 conserva il riferimento alla possibilità che, in cambio della fornitura di contenuti o servizi digitali, il consumatore fornisca i suoi dati personali.

È importante stabilire se un contratto è gratuito o oneroso perchè ci sono delle differenze in tema di disciplina applicabile e di tutela dell'apparato rimediale.[34] Il legislatore europeo e di conseguenza quello italiano ha risolto il problema, omettendo di prendere in considerazione la

[32] Disciplinati già dalla Direttiva 83/2011, per cui la nozione del 2019 non è nuova rispetto al tema dei contenuti digitali.

[33] G. Marchetti, S. Thobani, *La tutela contrattuale dei consumatori di contenuti e servizi digitali* cit., p. 40

[34] *Ivi*, p. 41

qualifica giuridica di questa tipologia di operazione: poco importa se è un contratto a titolo oneroso o gratuito, quello che è importante è dire che il consumatore ha una tutela anche qualora, anziché pagare il prezzo, presta il consenso al trattamento dei propri dati personali.

A tal proposito, il legislatore europeo ha esteso ai fruitori di contenuti e servizi digitali solo apparentemente gratuiti la disciplina prevista per i contratti di fornitura di contenuti e servizi digitali; questo perché il consumatore, in cambio della fornitura di tali contenuti o servizi, offre una risorsa comunque traducibile in valore economico, ossia i suoi dati personali.

Allo stesso tempo, il legislatore europeo omette di qualificare giuridicamente il fenomeno in termini di onerosità o gratuità, mentre si impegna a rimarcare che "la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce".

Per superare queste difficoltà teoriche, il legislatore europeo e il codice del consumo evitano di utilizzare il concetto di controprestazione, ma, come si può notare dal comma 4 dell'art. 135octies si parla solo di "caso in cui", senza nulla dire sulla natura giuridica dell'operazione che si realizza.

Si tratta di una soluzione puramente terminologica, atteso che il caso in cui il servizio viene erogato a fronte del trattamento dei dati personali è parificato, a livello di disciplina, a quello in cui la fornitura del servizio è prestata a fronte di un corrispettivo in denaro.

Il considerando 24 della direttiva 770/2019 evita che ciò comporti l'assenza di rimedi contrattuali per il consumatore: "*la presente direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali. La presente direttiva dovrebbe pertanto applicarsi ai contratti in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o servizi digitali al consumatore e in cui il consumatore fornisce, o si impegna a fornire, dati personali*".[35]

In questa prospettiva, la posizione del consumatore che cede i suoi dati personali è equiparata a quella di chi paga un prezzo in denaro. Tuttavia, rimane ancora aperta la questione riguardante la natura giuridica di questa specifica situazione.

Risulterà necessario, nel caso in cui il consumatore presti i suoi dati personali, coordinare la disciplina prevista dalla presente direttiva con la disciplina di valore superiore prevista, ovvero, del GDPR.

La direttiva 770 non si applica quando i dati personali forniti dal consumatore vengono trattati esclusivamente per scopi direttamente legati alla fornitura del contenuto o del servizio

[35] Considerando 24 della Direttiva 770/2019.

digitale, o per adempiere agli obblighi legali del professionista, senza che tali dati vengano utilizzati per scopi diversi da quelli previsti. Questa esclusione è giustificata dal fatto che, in questa situazione, il professionista non richiede i dati al fine di ottenere un vantaggio economico o di lucro, ma solo per scopi strettamente funzionali all'esecuzione del servizio o al rispetto degli obblighi legali.

Questo schema escluderebbe ogni profilo di corrispettività, il che giustifica il motivo per cui, inizialmente, il legislatore europeo ha escluso la possibilità per il consumatore di avvalersi dei rimedi per il difetto di conformità, avendo egli ricevuto la fornitura del contenuto o il servizio digitale senza sopportare alcun sacrificio.[36]

2.2 La tutela contrattuale riservata al consumatore di contenuti e servizi digitali

La tutela contrattuale del consumatore nei confronti dei contenuti e servizi digitali si basa principalmente su due categorie di rimedi: quelli previsti per il caso di mancata fornitura e quelli per il caso di difetto di conformità. È importante sottolineare che il consumatore può usufruire di tali rimedi sia nel caso in cui paghi un prezzo come corrispettivo per la fornitura di questi contenuti o servizi, sia nel caso in cui ceda i suoi dati personali in cambio.

La novità introdotta dal legislatore europeo, che è stata recepita nel codice del consumo aggiornato, consiste nel fatto che i concetti tradizionali di responsabilità per mancata fornitura e difetto di conformità sono stati estesi anche ai prodotti digitali. Oggetto di sua attenzione è stato, infatti, uno schema caratterizzato dalla corrispettività tra le prestazioni, ciò mira a garantire una protezione più completa e coerente per i consumatori in un contesto digitale in rapida evoluzione.

Per quanto concerne l'applicazione dell'art. 135 octies, sarà sempre necessario condurre un'analisi dettagliata per determinare se l'elemento della corrispettività sia presente o meno in ciascuna transazione conclusa. Nel caso in cui la fornitura di servizi digitali da parte del professionista dipenda dal consenso del consumatore per l'utilizzo dei propri dati personali, allora sarà considerata corrispettività e la legge sarà applicabile. D'altro canto, se il consenso al trattamento dei dati del consumatore è considerato facoltativo, non ci sarà corrispettività e di conseguenza la norma non sarà applicabile.

[36] G. Marchetti, S. Thobani, *La tutela contrattuale dei consumatori di contenuti e servizi digitali* cit., pp. 42, 43.

La presenza di un legame di corrispettività è cruciale anche in situazioni di revoca del consenso al trattamento da parte del consumatore. Se vi è corrispettività nelle prestazioni, la revoca del consenso avrà un impatto sul vincolo contrattuale, liberando il fornitore del servizio digitale dai suoi obblighi contrattuali. In questo scenario, il fornitore non sarà più tenuto a fornire il servizio precedentemente pattuito.

Al contrario, se non esiste una connessione diretta tra le prestazioni, anche in caso di revoca del consenso al trattamento dei dati personali, il professionista sarà comunque obbligato a continuare a fornire il servizio al consumatore.

Un'altra situazione che potrebbe influenzare il contratto in caso di un accordo basato su prestazioni corrispettive è l'inadempienza da parte del consumatore. Quest'ultimo potrebbe fornire dati non veritieri, imprecisi o non aggiornati. In questa circostanza, considerando la natura reciproca del rapporto contrattuale, si possono applicare i rimedi tradizionali contro l'inadempienza della prestazione.[37]

Va detto, anzitutto, che il contenuto o servizio digitale è conforme al contratto soltanto se sussistono determinati requisiti oggettivi e soggettivi, contenuti nell'art. 135 decies codice del consumo, che possiamo rispettivamente elencare; i requisiti soggettivi di conformità sono integrati se:

a) il contenuto o servizio digitale corrisponde alla descrizione, alla quantità e alla qualità prevista dal contratto e presenta la funzionalità, la compatibilità, l'interoperabilità e le altre caratteristiche previste dal contratto;
b) è idoneo ad ogni uso particolare voluto dal consumatore e che è stato da questi portato a conoscenza dell'operatore economico al più tardi al momento della conclusione del contratto e che l'operatore economico ha accettato;
c) è fornito con tutti gli accessori, le istruzioni, anche in materia di installazione, e l'assistenza ai clienti previsti dal contratto;
d) è aggiornato come previsto dal contratto.[38]

Per quanto riguarda i requisiti oggettivi, il contenuto o servizio digitale deve essere:

a) adeguato agli scopi per cui sarebbe abitualmente utilizzato un contenuto digitale o un servizio digitale del medesimo tipo;

[37] A. Musio, *Cessione di dati personali quale corrispettivo di contenuti o servizi digitali*, Rivisita Diritto di internet, 2021

[38] *Ivi*, p. 43

b) della quantità e presentare la qualità e le caratteristiche di prestazione, anche in materia di funzionalità, compatibilità, accessibilità, continuità e sicurezza, che si ritrovano abitualmente nei contenuti digitali o nei servizi digitali dello stesso tipo e che il consumatore può ragionevolmente aspettarsi
c) fornito, se del caso, insieme agli eventuali accessori e istruzioni che il consumatore può ragionevolmente aspettarsi di ricevere
d) conforme all'eventuale versione di prova o anteprima del contenuto digitale o del servizio digitale messa a disposizione dal professionista prima della conclusione del contratto.[39]

Anche l'errata integrazione può costituire difetto di conformità se:

- il prodotto è stato installato dal professionista
- il prodotto è stato installato dal consumatore sulla base delle istruzioni fornite dal professionista

In particolare, è importante individuare gli obblighi a capo del professionista durante il rapporto commerciale che intraprende con il consumatore.

Il professionista è obbligato a tenere informato il consumatore sugli aggiornamenti disponibili, anche di sicurezza, necessari al fine di mantenere la conformità del contenuto digitale o del servizio digitale, e a fornirglieli, nel periodo di tempo:

a) durante il quale il contenuto digitale o il servizio digitale deve essere fornito a norma del contratto, se questo prevede una fornitura continua per un determinato periodo di tempo; oppure
b) che il consumatore può ragionevolmente aspettarsi, date la tipologia e la finalità del contenuto digitale o del servizio digitale e tenendo conto delle circostanze e della natura del contratto, se questo prevede un unico atto di fornitura o una serie di singoli atti di fornitura.

Se il consumatore non installa entro un congruo termine gli aggiornamenti forniti dal professionista, quest'ultimo non è responsabile per qualsiasi difetto di conformità derivante unicamente dalla mancanza dell'aggiornamento pertinente, a condizione che:

a) il professionista abbia informato il consumatore della disponibilità dell'aggiornamento e delle conseguenze della mancata installazione dello stesso da parte del consumatore; e

[39] M. Martorana, *Fornitura di contenuti o servizi digitali: le modifiche al Codice del consumo*, Altalex, 2021

b) la mancata installazione o l'installazione errata dell'aggiornamento da parte del consumatore non è dovuta a carenze delle istruzioni di installazione fornite dal professionista.

Se il contratto prevede che il contenuto digitale o il servizio digitale sia fornito in modo continuativo per un determinato periodo di tempo, l'obbligo di assicurare la conformità del contenuto digitale o il servizio digitale permane per l'intera durata di tale periodo.

Non vi è difetto di conformità se, al momento della conclusione del contratto, il consumatore era stato specificamente informato del fatto che una caratteristica particolare del contenuto digitale o del servizio digitale si discostava dai requisiti oggettivi di conformità previsti da tali disposizioni e il consumatore ha espressamente e separatamente accettato tale scostamento al momento della conclusione del contratto.

Salvo diverso accordo tra le parti, il contenuto digitale o il servizio digitale è fornito nella versione più recente disponibile al momento della conclusione del contratto.[40]

2.2.1 Rimedi esperibili dal consumatore

È alla direttiva 771/2019 che si deve fare riferimento per la disciplina dei rimedi fruibili dal consumatore per il caso in cui i beni con elementi digitali presentino un difetto di conformità.

Questa previsione mira a garantire al consumatore il diritto di attivare i rimedi contrattuali anche se abbia "pagato" fornendo i propri dati personali in cambio di un servizio.

I difetti di conformità possono essere suddivisi in difetti soggettivi e difetti oggettivi. I difetti soggettivi si verificano quando il professionista viola gli impegni contrattuali che ha assunto con il consumatore, come ad esempio non aderire a specifici standard di sicurezza indicati nei termini e condizioni del servizio. D'altra parte, i difetti oggettivi sorgono quando il contenuto digitale o il servizio digitale fornito non è adeguato alle finalità per le quali solitamente un contenuto o un servizio di quel tipo viene utilizzato. Per esempio, se un'applicazione per gli acquisti online fornita da un professionista non adotta adeguate misure di sicurezza, esponendo così le informazioni sulla carta di credito del consumatore a malware o spyware, si tratta di un difetto oggettivo di conformità.

[40] Art. 135 undecies Codice del consumo.

Nel considerando (25) della direttiva 2019/770/UE, viene specificato che i rimedi contrattuali a favore dei consumatori per i difetti di conformità non si applicano ai servizi digitali o ai contenuti digitali gratuiti nei casi in cui la registrazione del consumatore è obbligatoria per motivi di sicurezza e identificazione, oppure quando il professionista raccoglie solo metadati come informazioni sul dispositivo o cronologia di navigazione. Inoltre, tali rimedi non si applicano se il consumatore è esposto a messaggi pubblicitari senza aver concluso un contratto con il professionista, ma solo per ottenere l'accesso ai contenuti digitali o a un servizio digitale.

Pertanto, è necessario che vi siano termini e condizioni per usufruire del servizio o accedere ai contenuti gratuiti. Allo stesso tempo, i dati personali del consumatore devono essere monetizzati in qualche modo, ovvero trattati per scopi commerciali di qualsiasi tipo, indipendentemente dalla base giuridica utilizzata, compreso il consenso del consumatore.[41]

Il consumatore avrà il diritto di far valere i rimedi previsti in caso di mancata fornitura o di difetto di conformità del servizio o del contenuto digitale, consistenti, innanzitutto, nell'invito da parte del consumatore a fornire il contenuto o il servizio digitale; se a seguito di ciò il professionista omette nuovamente di adempiere, il consumatore potrà chiedere la risoluzione del contratto[42], eliminando con efficacia retroattiva gli effetti del contratto. Il consumatore può risolvere immediatamente il contratto solo in due circostanze: se il professionista ha dichiarato o è evidente dalle circostanze del caso che non adempierà all'obbligazione di fornire il contenuto o servizio digitale e nel caso in cui il professionista non adempie entro il termine essenziale per il consumatore.

I rimedi di cui il consumatore può valersi per il difetto di conformità consistono nel ripristino della conformità del contenuto digitale o del servizio digitale, nella riduzione del prezzo (solo per il consumatore che paga in denaro) e nella risoluzione del contratto[43]; rimedi tra i quali esiste una gerarchia: in primo luogo, il consumatore ha diritto al ripristino della conformità, salvo ciò non sia impossibile o ponga a carico del professionista costi sproporzionati, tenuto conto di tutte le circostanze del caso e, in particolare del valore che il contenuto o servizio digitale avrebbe in assenza del difetto di conformità e dell'entità di

[41] D. Fulco, *Codice del consumo, Le nuove tutele privacy del 2022*, Network Digital 360, 2022

[42] Art. 13, direttiva 770/2019 e art. 135 septiesdecies cod. cons.

[43] Art. 14, direttiva 770/2014 e art. 135 octiesdecies cod. cons.

quest'ultimo. In queste due ipotesi il consumatore ha diritto all'immediata riduzione proporzionale del prezzo o alla risoluzione del contratto.

Il professionista rende il contenuto digitale o il servizio digitale conforme entro un congruo termine a partire dal momento in cui è stato informato dal consumatore in merito al difetto di conformità, senza spese e senza notevoli inconvenienti per il consumatore, tenuto conto della natura del contenuto digitale o del servizio digitale e dell'uso che il consumatore intendeva farne.[44]

Non è possibile azionare il rimedio della riduzione del prezzo se il consumatore ha fornito i suoi dati personali, perché, effettivamente, non ha pagato un prezzo, anche se il trattamento dei dati personali genera un valore economico per l'azienda.

Il consumatore ha diritto a una riduzione proporzionale del prezzo se il contenuto digitale o il servizio digitale è fornito in cambio del pagamento di un prezzo, o alla risoluzione del contratto, in uno dei casi seguenti:

a) il rimedio del ripristino della conformità del contenuto digitale o del servizio digitale è impossibile o sproporzionato;
b) il professionista non ha ripristinato la conformità del contenuto digitale o del servizio digita;
c) si manifesta un difetto di conformità, nonostante il tentativo del professionista di ripristinare la conformità del contenuto digitale o servizio digitale;
d) il difetto di conformità è talmente grave da giustificare un'immediata riduzione del prezzo o risoluzione del contratto; oppure
e) il professionista ha dichiarato, o risulta altrettanto chiaramente dalle circostanze, che non procederà al ripristino della conformità del contenuto digitale o del servizio digitale entro un congruo termine o senza notevoli inconvenienti per il consumatore.[45]

La riduzione del prezzo è proporzionale alla diminuzione di valore del contenuto digitale o del servizio digitale fornito al consumatore rispetto al valore che avrebbe se fosse stato conforme. Se il contratto stabilisce che il contenuto digitale o il servizio digitale deve essere fornito per un determinato periodo di tempo in cambio del pagamento di un prezzo, la riduzione di prezzo si applica al periodo di tempo in cui il contenuto digitale o il servizio digitale non è stato conforme.

[44]DECRETO LEGISLATIVO 4 novembre 2021, n. 173.

[45] S. Corongiu, *Contratti di fornitura di contenuto e di servizi digitali: le novità del d.lgs. n. 173/2021*, Altalex, 2021

Se il contenuto digitale o il servizio digitale è stato fornito in cambio del pagamento di un prezzo, il consumatore non ha diritto di risolvere il contratto se il difetto di conformità è di lieve entità, a differenza del caso in cui l'utente abbia fornito i suoi dati personali[46]. Questa diversità si spiega per il fatto che nel caso in cui il consumatore fornisca i suoi dati personali non ha diritto alla riduzione del prezzo e se il ripristino della conformità dovesse risultare impossibile o sproporzionato, il consumatore rimarrebbe sprovvisto di rimedi.

L'onere della prova riguardo al fatto che il difetto di conformità è di lieve entità è a carico del professionista, come anche l'onere della prova che in contenuto o servizio digitale soddisfi i requisiti di conformità.

Dopo la risoluzione del contratto, il professionista è tenuto a rimborsare al consumatore gli importi pagati in esecuzione del contratto. Tuttavia, se il consumatore ha fornito i suoi dati personali come parte del contratto, questa situazione si intreccia con le normative sulla protezione dei dati personali, previste dal GDPR e dal d.lgs. n. 101/2018.

Il professionista è responsabile solo per i difetti di conformità che si manifestano entro due anni a decorrere dal momento della fornitura e l'azione diretta a far valere i difetti sussistenti al momento della fornitura e non dolosamente occultati dal professionista si prescrive nel termine di ventisei mesi da tale momento, ove risultino evidenti entro tale termine.

Infine, per i contratti di fornitura continuata nel tempo[47], il professionista risponde se il difetto di conformità si manifesta nel periodo di tempo durante il quale il contenuto o servizio digitale deve essere fornito.[48]

[46] Art. 14, n.6, direttiva 770/2019 e art. 135 octiesdecies cod. cons., ultimo comma.

[47] Art. 11. Direttiva 770/2019 e art. 135 quaterdecies cod.cons.

[48] G. Marchetti, S. Thobani, *La tutela contrattuale dei consumatori di contenuti e servizi digitali* cit., pp. 45, 46.

CAPITOLO III

CASO FACEBOOK V. AGCM

Nel novembre 2018, l'Autorità Garante della Concorrenza e del Mercato (AGCM) ha emesso una delibera (n. 27432 del 29 novembre 2018) di sanzione nei confronti di Facebook Inc. e Facebook Ireland Ltd., imponendo loro una multa amministrativa di dieci milioni di euro. Questa sanzione è stata applicata in relazione a due presunte pratiche commerciali "scorrette" che coinvolgevano il trattamento dei dati personali degli utenti di Facebook. Tali pratiche si sono verificate sia durante la fase di registrazione degli account degli utenti che durante l'utilizzo dei servizi offerti dalla piattaforma.

L'AGCM ha basato la sua decisione sulla presunta violazione degli articoli 20[49], 21, 22, 24 e 25 del decreto legislativo n. 206/05, noto come il "Codice del Consumo". La sanzione è stata determinata prendendo in considerazione sia la gravità delle violazioni che la loro durata.

In particolare, le pratiche commerciali in questione hanno coinvolto la raccolta, l'impiego e la condivisione con terze parti dei dati personali degli utenti - consumatori, a scopi di natura commerciale. Insieme ai dati personali, sono stati oggetto di utilizzo e scambio anche gli interessi manifestati dai membri della piattaforma di social networking nel corso del tempo.

3. Le questioni giuridiche sollevate

La prima delle due condotte contestate, definita "ingannevole"[50] dall'AGCM, riguardava l'informativa fornita da Facebook durante la prima fase di registrazione degli utenti.

[49] L'art. 20 secondo comma del Codice del Consumo stabilisce precisamente che: "*una pratica commerciale è scorretta se è contraria alla diligenza professionale, ed è falsa o idonea a falsare in misura apprezzabile il comportamento economico, in relazione al prodotto, del consumatore medio che essa raggiunge o al quale è diretta o del membro medio di un gruppo qualora la pratica commerciale sia diretta a un determinato gruppo di consumatori*".

[50] Precisamente, nella delibera dell'Agcm si legge che*: "Facebook non informa l'utente con chiarezza e immediatezza in merito alla raccolta e all'utilizzo, a fini remunerativi, dei dati dell'utente da parte del Professionista e, conseguentemente, dell'intento commerciale perseguito, volto alla monetizzazione dei medesimi. Le informazioni fornite risultano generiche ed incomplete senza adeguatamente distinguere tra, da un lato, l'utilizzo dei dati funzionale alla personalizzazione del servizio con l'obiettivo di facilitare la socializzazione con altri utenti "consumatori", dall'altro, l'utilizzo dei dati per realizzare campagne pubblicitarie mirate. L'ingannevolezza risulta, peraltro, aggravata dalla circostanza che, nell'uso di FB, le*

L'AGCM ha affermato che questa informativa non era adeguatamente chiara nel comunicare agli utenti come i loro dati personali sarebbero stati utilizzati dalla piattaforma, ma era orientata principalmente alla loro acquisizione, utilizzo e/o la condivisione con terzi a scopi puramente commerciali.

L'informativa, presente sulla pagina di registrazione, faceva intendere che l'uso del servizio fosse gratuito e non menzionava in modo esplicito gli scopi commerciali legati al trattamento dei dati personali. L'AGCM ha concluso che questa informativa mancasse di chiarezza, immediatezza e completezza, il che ha reso difficile per gli utenti comprendere appieno le finalità commerciali che sottendevano la fornitura del servizio di social network[51].

Nel tentativo di affrontare questa violazione, l'AGCM ha imposto un divieto a Facebook di ripetere tale comportamento ingannevole. Inoltre, è stata richiesta la pubblicazione di una dichiarazione rettificativa dell'informativa, come previsto dall'articolo 27, comma 8[52], del Codice del Consumo, entro quarantacinque giorni dalla notifica del provvedimento. Questa dichiarazione doveva essere visibile sulla homepage del sito web aziendale di Facebook in Italia e sull'app Facebook per un periodo di venti giorni, a partire dalla mezzanotte del quarantacinquesimo giorno successivo alla notifica del provvedimento.[53]

La seconda condotta, definita "aggressiva"[54] dall'AGCM, riguardava il trasferimento dei dati degli utenti da Facebook ad altre applicazioni o siti web di terzi con finalità commerciali, senza ottenere il preventivo consenso esplicito degli utenti.[55]

---

finalità commerciali si prestano ad essere confuse con le finalità sociali e culturali, tipiche di un social network. Nella pagina di registrazione a FB, a fronte del claim "Facebook ti aiuta a connetterti e rimanere in contatto con le persone della tua vita", rileva, dunque, l'assenza di un adeguato alert che informi gli utenti, con immediatezza ed efficacia, in merito alla centralità del valore commerciale dei propri dati rispetto al servizio di social network offerto, limitandosi FB a sottolineare come l'iscrizione sia gratuita per sempre. L'incompletezza dell'informazione fornita nella pagina di accesso a Facebook non viene meno neanche per la recente introduzione, da aprile 2018, del "banner cookie" in quanto la sua visualizzazione è solo eventuale e non necessariamente collegata alla registrazione nella Piattaforma FB".

[51] Come da delibera Agcm n. 27432/18, pratica a), n. 4.

[52] Il quale dispone che: "*L'Autorità, se ritiene la pratica commerciale scorretta, vieta la diffusione, qualora non ancora portata a conoscenza del pubblico, o la continuazione, qualora la pratica sia già iniziata. Con il medesimo provvedimento può essere disposta, a cura e spese del professionista, la pubblicazione della delibera, anche per estratto, ovvero di un'apposita dichiarazione rettificativa, in modo da impedire che le pratiche commerciali scorrette continuino a produrre effetti*".

[53] "Facebook-raccolta utilizzo dati degli utenti", www.agcm.it.

[54] In relazione a tale seconda condotta l'Autorità ha deliberato che: "*la pratica commerciale descritta nella sezione II sub b), risulta aggressiva in quanto, mediante indebito condizionamento, è da ritenersi idonea a limitare considerevolmente la libertà di scelta o di comportamento del consumatore medio inducendolo, pertanto, ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso, nello specifico, la decisione di integrare le funzionalità della Piattaforma FB (sito web e app) con quelle di siti web/app di terzi, inclusi i giochi, e di trasferire, conseguentemente, i propri dati da FB a terzi e viceversa. Diversamente da quanto eccepito dal professionista, tale pratica è strutturalmente autonoma rispetto alla pratica sub a) in quanto relativa ad una scelta di consumo distinta".*

[55] Come previsto dall'art. 7 del Regolamento UE 2016/679 (GDPR).

A tal riguardo, è emersa una crescente preoccupazione riguardo alla protezione dei dati personali nell'ambito delle interazioni tra diverse piattaforme digitali, come quelle gestite da Facebook, tra cui WhatsApp, Messenger e Instagram. Diverse analisi condotte da esperti hanno evidenziato come l'interazione tra queste diverse piattaforme, sebbene siano tutte di proprietà dello stesso titolare, possa comportare conseguenze preoccupanti per la tutela dei dati personali.

Nel processo di "esternalizzazione" dei dati, delle informazioni e degli interessi degli utenti tra queste piattaforme, esiste la possibilità che tali dati vengano analizzati da sistemi di intelligenza artificiale con l'obiettivo di perseguire finalità di marketing.

3.1 La decisione del TAR Lazio

In questa situazione, il TAR Lazio (Tribunale Amministrativo Regionale del Lazio) ha accolto parzialmente il ricorso presentato da Facebook contro la delibera dell'AGCM, riconoscendo come fondata esclusivamente la prima delle due pratiche contestate e rigettando invece la seconda poiché priva di fondamento.

Quando si è esaminata la prima condotta, la cui validità è stata confermata dai Giudici Amministrativi, è stato preso in considerazione la richiesta ("claim") di Facebook che appare sulla pagina di registrazione iniziale e che invita gli utenti a iscriversi con la promessa che "Iscriviti, è gratis e lo sarà per sempre".

Questa promessa sembrava suggerire agli utenti che non ci fosse alcuna controprestazione "contrattuale" richiesta per utilizzare il social network, ma che la fruizione del servizio fosse completamente libera e gratuita.

Tuttavia, secondo quanto stabilito dal TAR Lazio, non è corretto considerare questo servizio come effettivamente gratuito, alla luce degli obiettivi che Facebook perseguiva attraverso l'uso dei dati personali dei suoi iscritti.

Il TAR Lazio ha sostenuto la decisione dell'AGCM, sottolineando la mancanza di completezza e chiarezza nelle informazioni fornite agli utenti. Questa mancanza di trasparenza aveva impedito agli utenti di comprendere appieno come i loro dati sarebbero stati utilizzati, e ciò che era essenziale rendere immediatamente chiaro.

Il tribunale ha affermato che questa pratica era effettivamente ingannevole e aveva impedito agli utenti di prendere decisioni consapevoli, nascondendo loro il valore economico che la società otteneva dalla registrazione al social network.

Al contrario, non è stata accettata l'argomentazione di Facebook basata sull'idea che il servizio fosse gratuito, giustificata dalla mancanza di un pagamento in denaro richiesto. Di conseguenza, a Facebook è stato ordinato di pubblicare una dichiarazione rettificativa sull'informativa presente sul suo sito web.

La seconda condotta sanzionata dall'Autorità, relativa al meccanismo di integrazione tra diverse app e social network, è stata valutata in modo diverso dai Giudici Amministrativi:

hanno ritenuto che questa pratica non violasse i diritti degli utenti e hanno eliminato la sanzione pecuniaria associata ad essa.

A conseguenza di ciò, la multa originariamente di dieci milioni di euro è stata ridotta a cinque milioni di euro.

Il TAR ha giustificato questa decisione sostenendo che, al momento della registrazione su Facebook, gli utenti avevano la possibilità di fornire il proprio consenso riguardo all'utilizzo dei loro dati personali in caso di integrazioni con altre piattaforme. Pertanto, il TAR ha concluso che non vi fossero elementi sufficienti a dimostrare che gli utenti fossero stati condizionati indebitamente in questo processo.

3.2 La class action di Altroconsumo

Il tribunale ha dato ragione alla class action intentata da Altroconsumo[56], che aveva segnalato ufficialmente il comportamento del social network già a partire da maggio 2018, con lo scandalo Facebook-Cambridge Analytica, quando fu scoperto che la società di consulenza britannica aveva raccolto i dati personali di milioni di account Facebook senza il loro consenso e li aveva utilizzati per scopi di propaganda politica.

Altroconsumo, insieme ad associazioni di consumatori in Belgio, Spagna e Portogallo, ha reagito immediatamente inviando a Facebook una richiesta ufficiale di spiegazioni e impegni precisi.

Tuttavia, a seguito delle risposte insoddisfacenti fornite da Facebook, il 30 maggio 2018 fu ufficialmente lanciata una class action contro il social network. Questa azione legale mirava a ottenere un risarcimento per gli utenti coinvolti, considerando i benefici commerciali ottenuti da Facebook attraverso l'abuso dei dati dei propri utenti e le normative a tutela dei consumatori.

[56] "*Class action Facebook, sentenza storica del Tar: i nostri dati valgono*", www.altroconsumo.it, 2020.

In particolare, Altroconsumo richiese un risarcimento di 285 euro per ogni anno di iscrizione al social network per ciascun aderente.

3.3 I risvolti

Un aspetto significativo di queste decisioni del TAR riguarda il riconoscimento del valore economico e commerciale dei dati personali nel mercato digitale.

I Giudici Amministrativi, nonostante abbiano riconosciuto la fondatezza solo della prima delle due condotte contestate a Facebook, hanno posto un'enfasi significativa sull'importanza dei dati personali nell'ambito dell'utilizzo delle piattaforme web. In particolare, hanno sottolineato che i dati personali possono essere considerati come un "asset" o risorsa disponibile che ha un valore negoziabile e può essere sfruttato economicamente. Di conseguenza, questi dati personali possono essere considerati come una controprestazione[57] tecnica all'interno di un contratto.

In effetti, questa nuova prospettiva evidenziata dai Giudici Amministrativi sottolinea che i dati personali non sono solo un diritto inviolabile della personalità dell'individuo, ma rappresentano anche un bene che può essere oggetto di compravendita esistente tra gli operatori del mercato digitale per mezzo del social network e gli utenti.[58]

I dati personali vengono perciò considerati beni commerciali e controprestazioni contrattuali.

In conclusione, le decisioni del TAR hanno evidenziato che, nell'ambito della protezione dei dati personali degli utenti dei servizi di social network, la privacy da sola potrebbe non essere sufficiente. È fondamentale garantire una maggiore chiarezza riguardo all'utilizzo dei dati personali, data la loro crescente importanza come asset commerciali nei mercati digitali. Le pronunce del TAR hanno portato a una ridefinizione del significato dei dati personali e alla necessità di fornire informazioni complete ed esaustive agli utenti. In un'epoca in cui i dati personali hanno un valore economico crescente, queste decisioni giuridiche hanno aperto la

[57] Cfr. S. Thobani*, Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, media Laws, pp. 137 – 143.
[58] In particolare, la Direttiva UE 770/2019 ha evidenziato proprio il valore di scambio dei dati personali forniti dagli utenti per l'utilizzo dei servizi digitali, in cui vengono ricompresi tutti quei contratti di fornitura di contenuti digitali. "*I dati personali come asset negoziale*", www.meplaw.net, 2020.

strada a una maggiore protezione dei consumatori e a una maggiore trasparenza nel settore digitale.[59]

[59] S. Giancone, *Il caso Facebook c. AGCM: i dati personali sono controprestazioni contrattuali*, Ius in itinere, 2020.

CAPITOLO IV

CONSIDERAZIONI FINALI

La questione del "pagamento" mediante dati personali può essere esaminata da diverse prospettive.

Innanzitutto, si può guardare da vicino i singoli rapporti in cui avviene lo scambio tra dati personali e servizi. In questa prospettiva, le preoccupazioni principali riguardano la tutela dell'individuo interessato o consumatore e l'esito del singolo contratto. È importante notare che, per quanto riguarda la protezione dell'individuo, chiunque voglia interrompere il trattamento dei propri dati può farlo in qualsiasi momento revocando il consenso, senza dover dimostrare l'illegalità delle operazioni di "tying" (vincolo contrattuale tra dati e servizi)[60].

Per quanto riguarda la tutela del consumatore, chi ha acconsentito al trattamento dei dati per accedere a un servizio per il quale non è richiesta un'altra prestazione potrebbe non avere interesse a far valere i rimedi previsti in suo favore, come ad esempio chiedere la risoluzione del contratto o recedere dallo stesso.

Inoltre, la difficoltà di quantificare il valore dei dati e il fatto che l'interessato ha comunque usufruito di un servizio possono rendere complesso e poco efficace il tentativo di valutare le conseguenze in termini di restituzione o risarcimento in caso di operazioni illegali legate ai dati.

Tuttavia, è altrettanto importante considerare la prospettiva collettiva. Le normative sulla protezione dei dati personali mirano a limitare la grossa concentrazione e il trattamento massiccio di dati personali, poiché ciò può comportare rischi per l'intera società.

Le normative sulla protezione dei consumatori, d'altro canto, mirano a tutelare non solo il singolo consumatore ma anche il funzionamento del mercato nel suo complesso. In entrambi i casi, le regole agiscono a livello individuale per raggiungere risultati su scala collettiva[61].

[60] S. Thobani, *Il pagamento mediante dati personali* cit., p. 377

[61] *Ivi*, p. 378

È importante notare che queste due prospettive non possono essere considerate separatamente, poiché la massa di rapporti che la normativa mira a tutelare è comunque costituita da singoli rapporti. Le due prospettive si intrecciano e sono complementari[62].

L'analisi della doppia prospettiva di tutela del mercato e della protezione dei dati personali evidenzia un'ambivalenza nelle informazioni personali. Queste informazioni possono essere considerate sia come beni di natura economica che come oggetto di un diritto fondamentale. Questa ambivalenza è presente nella normativa sulla protezione dei dati personali, che mira a garantire sia la libera circolazione dei dati che la protezione degli interessati. Tuttavia, questa ambivalenza può portare a risultati contraddittori.

La normativa sulla protezione dei dati personali limita la raccolta dei dati e la possibilità di subordinare l'accesso a un bene o servizio alla prestazione del consenso al trattamento. D'altra parte, la normativa sulla protezione dei consumatori cerca di promuovere la trasparenza nelle operazioni di mercato, riconoscendo il legame tra servizi e dati personali. Questo può creare tensioni, poiché da un lato si limita la raccolta e il trattamento dei dati personali senza consenso, mentre dall'altro si cerca di garantire la trasparenza nell'uso di tali dati.

Il Garante europeo per la protezione dei dati personali ha rilevato questa contraddizione e ha contestato la qualifica dei dati personali come controprestazione[63] in alcune proposte legislative. La soluzione di compromesso raggiunta in alcune direttive cerca di bilanciare la protezione dei dati personali con la necessità di informare i consumatori sugli utilizzi dei loro dati, evitando di considerare i dati come una merce.

La soluzione di compromesso raggiunta nella versione finale della direttiva evita di utilizzare il termine "controprestazione" in relazione ai dati personali e afferma che i dati non possono essere considerati come una merce. Tuttavia, questa soluzione può essere vista come essenzialmente nominalistica, poiché, indipendentemente dalla qualifica formale dei dati come controprestazione, il caso in cui un servizio venga erogato in cambio del consenso al trattamento dei dati viene comunque equiparato, in termini di disciplina, a quello in cui è previsto un pagamento in denaro.

In altre parole, anche se la direttiva evita di definire i dati personali come una controprestazione, essa continua a trattare il servizio erogato in cambio del consenso al trattamento dei dati in modo simile a un servizio che viene pagato in denaro. Ciò significa che

---

[62] *Ivi*, p. 379

[63] Garante europeo per la protezione dei dati personali, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for supply of digital content*

le norme sulla protezione dei dati personali continuano a essere applicate in modo rigoroso, garantendo la privacy e i diritti degli individui, anche quando i dati personali sono utilizzati come parte di una transazione o per l'accesso a un servizio. La direttiva conferma la prevalenza della normativa sulla protezione dei dati personali in tali situazioni. In astratto, se un servizio o contenuto digitale viola norme essenziali del GDPR di natura comportamentale, il consumatore potrebbe avviare un'azione legale per annullare il contratto. Questa possibilità è contemplata anche nell'articolo 48 della direttiva 2019/770/UE, che tiene conto delle situazioni in cui il contratto può essere dichiarato nullo o annullabile secondo le leggi nazionali. In Italia, la giurisprudenza stabilisce che, se la violazione delle norme comportamentali essenziali comporta a un vizio della volontà nella formazione del consenso delle parti, il contratto può essere annullato.

Per affrontare questa contraddizione, è importante differenziare i diversi aspetti delle normative in questione. La disciplina sulla protezione dei dati regola sostanzialmente il mercato dei dati personali, stabilendo quando è ammesso lo scambio di tali dati. D'altra parte, la disciplina a tutela dei consumatori regola le modalità di questo scambio, garantendo la trasparenza e fornendo ai consumatori rimedi specifici, indipendentemente dalla liceità dello scambio.[64]

Il legislatore europeo, quindi, è guidato da due diverse spinte quando si tratta di regolare la gestione dei dati personali. Da un lato, vi è la spinta a tutelare il mercato, garantendo la trasparenza nelle operazioni che coinvolgono i dati personali e cercando di agevolarne la circolazione. Dall'altro lato, c'è la spinta a tutelare i diritti fondamentali degli individui, che porta a riconoscere l'esistenza di un'area di "non-mercato" in cui sono coinvolti valori indisponibili. La questione fondamentale è se i dati personali rientrino in questa "area di non-mercato". Come precedentemente argomentato, la risposta a questa domanda è negativa, nonostante si tratti di un mercato strettamente regolamentato.

Nella regolamentazione dei dati personali, il legislatore europeo ha scelto di limitare la possibilità di trattare i dati come risposta ai rischi associati al trattamento dei dati stessi. Questo si riflette nella definizione di requisiti rigorosi per la validità del consenso. Si tratta di un approccio che tenta di affrontare questioni che coinvolgono interessi superindividuali con strumenti di tutela dei singoli, che risultano così funzionalizzati a obiettivi esterni al singolo rapporto.

[64] S. Thobani, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, media Laws, p. 146

È importante riconoscere che questa soluzione potrebbe non essere la soluzione migliore per affrontare i rischi legati al trattamento dei dati personali.

Limitare la raccolta dei dati può non essere sufficiente per affrontare i rischi che si presentano dopo il trattamento dei dati, come la discriminazione. Un approccio più efficace potrebbe essere quello di affrontare i rischi a valle, aprendo un dibattito sulla definizione e l'ampliamento dei risultati discriminatori vietati. In questo senso, la fiducia eccessiva nel consenso individuale potrebbe non essere la soluzione ideale per affrontare i problemi legati alla protezione dei dati personali.[65]

[65] *Ivi*, p. 147

BIBLIOGRAFIA

S. Thobani, *Il pagamento mediante dati personali*, *Annuario 2021 Osservatorio Giuridico sulla Innovazione Digitale*, a cura di S. Orlando e G. Capaldo, Sapienza Università Editrice, 2021, pp. 361 ss.

C. Irti, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, spec. 45 ss.

F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018.

S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità, Europa e diritto privato 2/16*, Giuffrè Editore, 2016, pp. 513 ss.

S. Thobani., *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in Media Laws, 2019, pp. 131 ss.

G. Marchetti, S. Thobani, *La tutela contrattuale dei consumatori di contenuti e servizi digitali, Manuale di diritto privato delle nuove tecnologie*, a cura di G. Magri, S. Martinelli e S. Thobani, Giappichelli, 2022, pp. 35 ss.

E. Battelli, *I modelli negoziali di business degli operatori digitali a "prezzo zero" non sono gratuiti*, Altalex, 2022.

L. Berto, *Il Digital Single Market: di cosa tratta e che punto siamo*, Ius in itinere, 2018.

A. Musio*, Cessione di dati personali quale corrispettivo di contenuti o servizi digitali*, Rivisita Diritto di internet, 2021

M. Martorana, *Fornitura di contenuti o servizi digitali: le modifiche al Codice del consumo*, Altalex, 2021

D. Fulco, Codice del consumo, *Le nuove tutele privacy del 2022*, Network Digital 360, 2022

S. Corongiu, *Contratti di fornitura di contenuto e di servizi digitali: le novità del d.lgs. n. 173/2021*, Altalex, 2021

"Class action Facebook, sentenza storica del Tar: i nostri dati valgono", www.altroconsumo.it, 2020.

D. Fiori, *"Il TAR sulle sanzioni Antitrust",* www.assoutenti.it, 2020.

"*I dati personali come asset negoziale*", www.meplaw.net, 2020.

S. Giancone, *Il caso Facebook c. AGCM: i dati personali sono controprestazioni contrattuali*, Ius in itinere, 2020.