Internet Service Provider

Ruolo e responsabilità

Indice

PREMESSA

L'elaborato in questione ha lo scopo di analizzare l'evoluzione, il ruolo e soprattutto la responsabilità dell'Internet Service Provider nell'era digitale moderna.

L'Internet Service Provider è una figura (organizzazione o azienda) che fornisce accesso ad internet a tutti i suoi utenti, svolgendo una pluralità di servizi, quali ad es: connettività ad internet, accesso alla posta elettronica, navigazione su siti web e piattaforme digitali ed altro.

La crescente ubiquità di internet ha ridefinito il panorama della responsabilità legale, ponendo l'ISP al centro di dibattiti cruciali sulla tutela dei diritti digitali e la gestione di contenuti online.

Questa tesi avrà lo scopo di esplorare il ruolo e la posizione del provider difronte al sempre più diffuso fenomeno di internet e dei social network. Il problema giuridico odierno è quello di comprendere se e quando sia possibile imputare una responsabilità agli ISP nel momento in cui vengono compiute violazioni sulla rete direttamente o indirettamente, cioè da parte dei fruitori dei loro servizi; e ancor prima, capire come gli ISP possano affrontare ed evitare i rischi e le conseguenze che ne sono sottesi.

Al giorno d'oggi viviamo in un mondo iper-connesso, dove, ogni minuto, migliaia di notizie e contenuti vengono diffusi tramite social media o piattaforme digitali, creando una rete intensa e sofisticata. Il provider assume un ruolo cruciale nella gestione della moltitudine di contenuti che affollano la rete ogni giorno; la responsabilità del prestatore di servizi fa nascere infatti questioni complesse, spaziando dall'equilibrio tra la libertà di espressione e la necessità di controlli.

La tesi in questione si soffermerà anche su un'analisi del quadro normativo europeo che regolamenta l'ambito trattato, evidenziando la delicatezza e la continua evoluzione della materia in esame. Ciò che rappresenta, quindi, il cuore di questo elaborato riguarda la possibilità di poter considerare il provider responsabile, o meno, nel caso in cui vengano diffusi contenuti illeciti nella sua piattaforma o attraverso i servizi di intermediazione da esso forniti. Verranno, pertanto, trattati alcuni casi pratici di Giurisprudenza che hanno caratterizzato il nostro ordinamento e più in generale il panorama Europeo, soffermando l'attenzione anche sui recenti interventi normativi e sulle strategie politico-economiche adottate dall'Unione nell'ambito della creazione e regolamentazione di un mercato unico digitale.

PARTE I

1) Evoluzione dei social network e ruolo dell'I.S.P.

In questo primo capitolo verranno analizzati gli sviluppi storici, tecnologici e giuridici che hanno caratterizzato sino ad oggi il rapporto tra la nuova frontiera dei social network e la figura dell'internet service provider.

Si partirà prima di tutto da una ricostruzione storica della nascita e dell'evoluzione dell'internet service provider, del quale verranno trattate le caratteristiche principali e il suo rapporto con il nuovo mondo dell'internet e delle piattaforme digitali.

Seguirà poi una parentesi storica sull'evoluzione dei social network e del mondo digitale, analizzando l'impatto che queste nuove tecnologie hanno avuto sulla nostra società, sul nostro modo di vivere, di pensare e di agire.

Si arriverà infine ad un'elencazione dei benefici, ma soprattutto dei rischi che possono derivare dall'utilizzo dei social, ponendo principalmente l'attenzione sugli effetti sul pubblico dei giovani, i quali, nella maggior parte dei casi, possono subirne più di tutti le conseguenze.

1.1) Internet Service Provider, evoluzione e ruolo.

Si inizia a parlare di Internet Service Provider principalmente negli anni 90', periodo in cui la figura in questione viene qualificata come un mero operatore che esercita la sua attività attraverso l'utilizzo di banchi di modem [1].

Nei primi anni del XXI secolo, con l'esplosione dell'internet e dei primi social network, si assiste ad un'evoluzione esponenziale del ruolo e delle funzioni dei providers, i quali iniziano a ricoprire delle posizioni ben più importanti e significative rispetto a quelle citate precedentemente, divenendo figure chiave nell'accesso ad internet e nell'utilizzo dei servizi ad esso correlati.

Al giorno d'oggi l'ISP può essere definito come una figura che funge da organizzazione per la fornitura di servizi di accesso e di utilizzo di internet agli utenti. "*Si tratta in pratica di strutture, oramai commerciali, che, oltre all'accesso alla rete, garantiscono l'utilizzo dei servizi ad essa connessi, quali ad esempio registrazione, caselle di posta elettronica* […] [2]"

[1] Avv. F. Molinari, "nascita, evoluzione e funzionamento della rete", Diritto.it, 2008

[2] Avv. F. Molinari, "nascita, evoluzione e funzionamento della rete", Diritto.it, 2008, nota 38;

Agli albori della rete esistevano, come ovvio, pochi internet service providers; uno tra i primi è stato: "*America Online*[3]*",* una compagnia che forniva accesso limitato ad internet attraverso connessioni di tipo "*dial-up*[4]*"* tramite le linee telefoniche.
Durante questa prima fase della rete internet si potevano elencare tre diverse tipologie di ISP, le seguenti:

- ISP che utilizzavano servizi di tipo dial-up, i quali garantivano una connessione alla rete attraverso l'utilizzo di modem e tramite la composizione di una normale numerazione telefonica, andati poi a diminuire nel corso del tempo a causa della scarsa velocità delle connessioni offerte;
- DSL dei provider telefonici, ossia una categoria di providers che utilizzavano le linee telefoniche per fornire le connessioni ad internet e si differenziavano dagli ISP che utilizzavano i servizi di tipo dial-up poiché in questo caso le informazioni venivano trasmesse non attraverso le chiamate bensì attraverso i cavi telefonici in rame. Si tratta di una tipologia di servizi che ha riscosso molto successo ai suoi tempi, vista la presenza di reti cablate per le linee telefoniche all'interno delle case che ha reso più facile la diffusione di queste connessioni;
- ISP che utilizzavano la banda larga e le connessioni via cavo, ossia quelle società che fornivano la connessione di servizi internet e tv via cavo tramite l'utilizzo di cavi a banda larga, i quali fornivano numerosi vantaggi, tra cui:
    a) Una bassa latenza che permette di non influire in maniera negativa sulla connessione dell'utente durante lo svolgimento delle proprie attività on-line;
    b) Un costo minore, consentendo di abbinare più servizi insieme, come appunto la tv via cavo e la connessione ad internet;
    c) Ampia disponibilità e diffusione.

[3] America Online, anche conosciuta con l'acronimo "AOL", è stata una società statunitense di servizi in rete, fondata nel 1985 e affermatasi nel 1990 come il più grande internet service provider del mondo, raggiungendo circa trenta milioni di utenti in tutto il globo. La società in questione è poi stata acquisita da Verizon nel 2015 ed è poi confluita nel gruppo Apollo Global Mnagement nel 2021.
[4] Per Dial-up si intende: Connessione alla rete che viene stabilita attraverso una chiamata telefonica, un sistema di comunicazione che utilizza quindi le linee telefoniche e non si appoggia a linee dedicate. Un esempio è la connessione via Modem a 56k.

Al giorno d'oggi, la modalità di connessione maggiormente diffusa in Europa e in altre parti del mondo, è quella in fibra ottica, la quale garantisce alcuni benefici, ossia:

- Un'elevata velocità di esecuzione e di svolgimento dei servizi;
- Immunità alle interferenze elettromagnetiche;
- Consistenza e affidabilità;
- Larghezza di banda e segnali di trasmissione più estesi.

Tornando alla figura del provider, la normativa che va a regolamentare l'attività e il ruolo dell'ISP, all'interno dell'Unione Europea, nasce in seno alla Direttiva n. 31/2000, recepita dal nostro ordinamento con il D.lgs. 70/2003.

Prima della normativa in questione, in Europa, era presente uno scenario frammentato riguardo la regolamentazione degli internet service provider; non esisteva infatti una normativa europea specifica che regolamentasse in maniera dettagliata la figura e il ruolo degli ISP.

La regolamentazione antecedente alla Direttiva n. 31/2000 era principalmente affidata alle legislazioni nazionali dei singoli paesi membri dell'Unione Europea, questo comportava di conseguenza una variazione notevole delle interpretazioni che ogni stato poteva dare nei confronti della materia in questione.

Come sostiene una parte della dottrina [5]: "*regole diverse a carico dei providers avrebbero ostacolato il processo espansivo dei traffici online*".

La Direttiva n. 31/2000 è stata introdotta dal legislatore europeo, non solo per disciplinare il commercio elettronico, ma anche con lo scopo di dare una maggiore uniformità nella regolamentazione della figura, del ruolo e della responsabilità del provider.

La normativa europea adotta il sistema dell'exemptions del provider [6], calibrate sulla ormai consolidata tassonomia dei servizi erogati dai provider, quali: mere conduit, caching e hosting, i quali verranno affrontati nel capitolo successivo.

[5] P. Sanna, Il regime di responsabilità dei providers intermediari di servizi della società dell'informazione, Milano, Giuffrè Editore, 2004, pp. 279-302.

[6] G.M. Riccio; la responsabilità degli internet service provider, situazione legislativa e problemi aperti, in V. D'antonio; S.vigliar, studi di diritto della comunicazione, persone, società e tecnologie dell'informazione, Padova, Cedam, 2009;

La scelta del legislatore, di regolamentare la responsabilità del provider in un'unica Direttiva, potrebbe essere quindi giustificata dall'esigenza di delineare un quadro giuridico chiaro ed uniforme in ambito europeo, data l'importanza che tale soggetto riveste all'interno del commercio elettronico [7].

Le funzioni svolte dagli ISP (come si vedrà anche nel capitolo successivo) sono plurime e di estrema importanza, in quanto queste figure hanno contribuito in maniera significativa allo sviluppo dell'era digitale in cui viviamo oggi.

Con il tempo, gli ISP sono diventati, loro malgrado, protagonisti di numerosi contenziosi sia dal punto di vista della tutela dei diritti di proprietà intellettuale sia con riferimento alla loro responsabilità civile.

Il problema giuridico odierno è quello di comprendere se e quando sia possibile imputare una responsabilità agli ISP nel momento in cui vengono compiute violazioni sulla rete direttamente o indirettamente, cioè da parte dei fruitori dei loro servizi; e ancor prima, capire come gli ISP possano affrontare ed evitare i rischi e le conseguenze che ne sono sottesi.

1.2) Evoluzione dei social network

Quando si parla di "social network" spesso si cade nell'errore di pensare a questo come a qualcosa di moderno e recente; in realtà il termine in questione ha origini molto più lontane di quanto si pensi.

La concezione moderna del temine "social network", inteso come una piattaforma digitale nella quale gli utenti interagiscono attraverso una connessione internet, viene utilizzato per la prima volta nel 2002 in seguito alla creazione di Friendster, un sito di incontri, nato da un'idea di Jonathan Abrams, con lo scopo di far interagire online le persone, garantendo ad esse la massima sicurezza [8].

Friendster non è stato considerato a tutti gli effetti un social network, quanto più un sito in cui gli utenti potevano interagire tra loro e creare nuove reti di conoscenze.

[7] M. De Cata, la responsabilità civile dell'internet service provider, Milano, Giuffrè Editore, 2010;

[8] D. M. Boyd; N. B. Ellison, social network sites: definition, history, and scholarship; Journal of Computer-Mediated communication, Vol. 13, issue 1, 2007, pag. 210-230;

Il primo vero e proprio social ad essere mai stato inventato prende il nome di "Sixdegrees", creato nel 1996 da Andrew Weinreich, con la funzione di mettere in contatto più utenti tra loro in una piattaforma digitale [9].

Negli anni successivi si è verificata un'espansione del web e della connessione via internet che ha portato, conseguentemente, alla nascita di numerosi social media, quali ad es: Facebook, Myspace, Youtube, Instagram […]

Si è assistito, recentemente, ad un incremento esponenziale di profili social e account online, i quali hanno avuto un impatto a dir poco notevole sulla nostra società e sulle nostre vite personali, basti pensare che solamente in Italia, su una popolazione netta di circa sessanta milioni di persone, più di cinquanta milioni utilizzano una connessione internet e circa quaranta milioni usano attivamente un social [10].

Con l'espressione "*social network"* si identifica, al giorno d'oggi: "*un servizio informatico online che permette la realizzazione di reti sociali virtuali. Si tratta di siti internet o tecnologie che consentono agli utenti di condividere contenuti testuali, immagini, video e audio e di interagire tra loro*[11]".

Questa definizione delinea le caratteristiche principali dei social network, quali la realizzazione di una rete virtuale, la possibilità di condivisione dei contenuti e la possibilità di analizzare quelli altrui.

Interessante anche la definizione riportata da uno studio del 2007 pubblicato nel Journal of computer-mediated communications, secondo il quale i social network possono essere descritti come segue: "*web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site* [12]."

Generalmente, il funzionamento dei social media si basa sulla registrazione dell'utente nella piattaforma digitale attraverso la creazione di un profilo personale, il quale viene visto come una proiezione dell'identità del soggetto nel mondo virtuale, che gli permette

---

[9] vedi nota precedente;

[10] Linkedin Italia, https://it.linkedin.com/pulse/i-numeri-dei-social-network-italia-nel-2023-indagine, 2023;

[11] Treccani, enciclopedia online; https://www.treccani.it/enciclopedia/social-network/;

[12] D. M. Boyd; N. B. Ellison, social network sites: definition, history, and scholarship; Journal of Computer-Mediated communication, Vol. 13, issue 1, 2007, pag. 210-230;

di essere riconosciuto da amici, familiari e utenti in generale, e di condividere con essi contenuti e messaggi vari; i social, quindi, non solo accorciano le distanze geografiche tra gli utenti, ma anche quelle temporali.
Tra i social maggiormente utilizzati figurano i seguenti [13]:

- Facebook, uno dei primi e dei più conosciuti social al mondo, creato nel 2004 e con quasi tre miliardi di utenti attivi ogni mese, racchiudendo quindi circa il 40% della popolazione mondiale;
- Youtube, una piattaforma web 2.0 fondata in California nel 2005 che permette la condivisione e la visualizzazione in rete di contenuti multimediali, con un numero di utenti attivi mensilmente pari a circa due miliardi e mezzo;
- Whatsapp, la più famosa piattaforma di messaggistica istantanea al mondo, con un totale di due miliardi di utenti attivi ogni mese;
- Instagram, colosso social sviluppato nel 2010 e di proprietà della società Meta (che detiene anche Facebook, whatsapp e Facebook messenger), con circa due miliardi di utenti attivi ogni mese;
- Tiktok, colosso cinese, uno dei social più recenti e popolari, diffuso specialmente tra i giovani, con circa un miliardo di utenti attivi mensilmente.

Il successo e l'esponenziale diffusione dei social ha portato il fenomeno in questione a diventare parte integrante della vita della maggior parte della popolazione mondiale.
Sono molti però i rischi e i pericoli legati all'utilizzo di questi strumenti, i quali spesso vengono sottovalutati o addirittura messi da parte dagli utenti.

1.2.1) opportunità e rischi legati all'utilizzo dei social.

Come affermato nel capitolo precedente, i social network e le piattaforme digitali hanno mutato in maniera radicale la nostra società, con evidenti effetti sia sulle vecchie che sulle nuove generazioni.

[13]Linkedin Italia, https://it.linkedin.com/pulse/i-numeri-dei-social-network-italia-nel-2023-indagine, 2023;

L'analisi riportata in questo paragrafo è finalizzata ad evidenziare tutti i possibili rischi e tutte le opportunità che i social e le piattaforme digitali possono generare nei confronti di chi li utilizza.

- Ampliamento delle conoscenze da parte degli utenti.

  Un utente, attraverso un social media, ha la possibilità di ampliare, in maniera esponenziale, la sua rete di conoscenze e di amicizie virtuali.

  Si tratta di una delle funzioni maggiormente apprezzate, tra quelle offerte dai social, perché contribuisce ad aumentare la creazione di nuove amicizie da parte degli utenti.

  Il rischio a cui può condurre la funzione qui elencata è rappresentato dal fatto che molti utenti rischiano, spesso senza neanche rendersene conto, di perdere il contatto fisico con la realtà.

  Alcune persone che interagiscono sui social spesso creano una rete molto fitta di amicizie virtuali con utenti di tutto il mondo, trascurando però quelle reali e fisiche e, conseguentemente, perdendo il contatto con il mondo reale.

  Alcuni utenti hanno infatti dichiarato espressamente che, attraverso i social, hanno effettivamente trascurato la loro vita fisica e le vere amicizie, rifugiandosi in un mondo virtuale che garantisce sicuramente un elevato numero di conoscenze e di libertà, ma si tratta pur sempre di un ambiente inventato e irreale, con amicizie occasionali, non vere e a distanza, nella maggior parte dei casi;

- Aumento dell'informazione generale.

  L'argomento in questione rappresenta uno dei più grandi benefici offerti dai social network e dal mondo delle piattaforme digitali poiché, grazie alla diffusione di informazioni, notizie e contenuti di cultura generale, gli utenti hanno la possibilità di apprendere nuove cose e di tenersi aggiornati su molti argomenti; basti pensare che, solamente negli Stati Uniti, i social vengono utilizzati come mezzo di informazione da circa il 67% della popolazione [14].

  Negli ultimi anni, precisamente dal 2019 ad oggi, secondo un'analisi fornita dal "*Censis*[15]", in Italia si è registrato un aumento dell'utilizzo dei social media come

[14] Ansa, "USA, due terzi delle persone leggono notizie sui social", su Ansa.it, 2017;

[15] Il Censis è un istituto di ricerca socioeconomica, fondato in Italia nel 1964, che si occupa di fornire sondaggi, censimenti, consulenze e analisi socioeconomiche.

strumento per reperire notizie ed informazioni riguardo il fenomeno del Covid-19; infatti, circa il 30% della popolazione italiana ha acquisito informazioni sulla pandemia attraverso l'utilizzo di social come Instagram, Facebook o Twitter.

Questo modo di agire porta, in determinate occasioni, gli utenti ad un continuo bisogno di reperire informazioni, notizie e tematiche di attualità dai social, facendone spesso un utilizzo spropositato.

Il fenomeno appena menzionato è conosciuto con il nome di: "*fear of missing out* [16]", ossia la paura di essere tagliati fuori, di essere messi in disparte dalla società e di non rimanere aggiornati su tutto quello che succede.

Il rischio che si annida dietro questo fenomeno è rappresentato, non solo da un abuso dell'utilizzo di questi social media e dalla nascita di preoccupazioni come quella precedentemente menzionata, ma anche dalla presenza e dall'enorme diffusione delle c.d. "*fake news* [17]" all'interno di queste piattaforme.

Spesso gli utenti, specialmente quelli con un'età maggiore, non riescono a distinguere un'informazione vera da una fake news, ossia una notizia non vera o in parte inventata, creata con lo scopo di ingannare i lettori.

Da un rapporto pubblicato dall'Oxford Internet Institute, chiamato "*digital news report 2021*[18]", il fenomeno delle fake news nel mondo dei social network aumenta di anno in anno. Da questa analisi si evince che la piattaforma all'interno della quale circolano la maggior parte delle notizie false è Facebook.

---

[16] La Fear of missing out, anche conosciuta con l'acronimo di FOMO, indica una forma di ansia sociale caratterizzata dal desiderio e dal bisogno di rimanere continuamente in contatto con le attività che vengono compiute dalle altre persone, e dalla paura di essere esclusi da eventi, esperienze e contesti sociali gratificanti. Si tratta di un fenomeno abbastanza recente che si è sviluppato parallelamente con i social network e le piattaforme digitali e che ha colpito principalmente il pubblico adolescenziale.

[17] Le fake news sono delle informazioni false e/o fuorvianti che possono essere divulgate attraverso qualsiasi media, allo scopo di produrre misinformazione o disinformazione. Il fenomeno delle fake news ha origini molto antiche che risalgono addirittura all'Antica Grecia, ma ad oggi, con l'avvento delle nuove tecnologie, in particolare i social media, la gente viene continuamente messa di fronte ad un'enorme mole di notizie e spesso si trova a decidere in fretta se queste siano vere oppure no. Il compito di ogni destinatario dell'informazione dovrebbe, per questo, essere quello di migliorare la propria abilità critica per distinguere le fonti affidabili da quelle che possono, più o meno intenzionalmente, diffondere false informazioni, effettuando controlli incrociati tra ciò che si legge e/o si sente e fonti riconosciute come affidabili.

[18] N. Newman; R. Fletcher; A. Schulz; S. Andi; C.T. Robertson; R.K. Nielsen,"Digital news report 2021", Reuters Institute for the study of journalism, X Edizione., Università di Oxford, 2021;

Le conseguenze più gravi che possono derivare dal fenomeno in questione sono: una disinformazione generale da parte degli utenti e un danneggiamento alla reputazione delle piattaforme stesse e dei loro vertici.

- Velocità di comunicazione e di diffusione di contenuti.

  Parte del successo di cui godono i social network al giorno d'oggi è rappresentata dalla velocità di comunicazione e dalla rapidità di diffusione di contenuti e messaggi.

  Attraverso l'utilizzo di queste piattaforme gli utenti possono interagire tra loro in maniera istantanea, connettendosi ad ogni luogo o parte del mondo senza alcun problema; come detto in precedenza, i social accorciano sia i tempi che le distanze geografiche, garantendo una diretta connessione tra gli utenti.

  Si tratta naturalmente di una funzione per così dire rivoluzionaria, che ha cambiato del tutto il mondo della messaggistica, portandolo ad un livello nettamente superiore rispetto a quello che c'era precedentemente, e quello della diffusione di informazioni, basti pensare che ogni giorno, solamente su Instagram, vengono caricati circa cento milioni di contenuti, con un numero di utenti attivi che va oltre un miliardo.

  Il rischio principale legato a questa funzionalità è rappresentato dall'enorme quantità di contenuti illeciti e messaggi discriminatori che vengono diffusi ogni giorno sui social.

  A causa della rapidità nella diffusione dei contenuti e dell'enorme quantità di questi, rimane difficile, sé non impossibile, eseguire un controllo atto a verificare la liceità di ognuno di essi; questo comporta sicuramente un incremento dei reati che vengono compiuti online, come ad es: il "*cyberbullismo*[19]", il "*revenge porn*[20]" e

[19] La definizione di cyberbullismo è stata introdotta per la prima volta con la L. n. 21/2019. Per cyberbullismo si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo;

[20] il fenomeno del "revenge porn", anche conosciuto con il termine "revenge pornography", fa riferimento alla condivisione pubblica di immagini o video intimi mediante Internet senza il consenso del protagonista degli stessi. Il più delle volte le registrazioni sono state eseguite ab origine con il consenso della vittima, ma vengono poi diffusi contro la volontà di quest'ultima. La pubblicazione delle immagini o delle registrazioni avviene solitamente al solo scopo di umiliare la persona coinvolta, per ritorsione o vendetta. A tal

la "*diffamazione online*[21]".

Si tratta di un fenomeno intorno al quale si è discusso molto, specialmente con riferimento al ruolo del provider e alla sua responsabilità in situazioni del genere; come si vedrà nei capitoli successivi, si tende generalmente ad escludere, a determinate condizioni, l'obbligo, in capo agli ISP, di una sorveglianza totale su ogni singolo contenuto che viene da essi veicolato o memorizzato.

- Possibilità di trarre profitto dall'utilizzo dei social.

  Sé in passato, agli albori dei primi social network, la possibilità di trarre profitto attraverso il loro utilizzo veniva considerato come qualcosa di utopico o addirittura impossibile, al giorno d'oggi può essere ritenuto un fenomeno più che concreto. Grazie all'utilizzo di piattaforme online come Instagram, Twitter o Facebook, personaggi famosi e influenti riescono a guadagnare cifre esorbitanti mediante la semplice condivisione di post pubblicitari.

  Guadagnare, quindi, attraverso l'utilizzo dei social, non solo è diventato qualcosa di concreto e reale, ma anche un'aspirazione per molte persone che tentano di acquisire notorietà e ricchezza su queste piattaforme mediante la pubblicazione di video e foto, oppure tramite l'avviamento di business online e siti di e-commerce. Tale aumento di ricchezza e di possibilità economiche sul mondo dei social, ha portato però anche ad un aumento esponenziale dei reati contro il patrimonio nel cyberspazio, quali ad es: "truffe informatiche [22]", "furti di identità digitale [23]" ed altre simili fattispecie[24].

---

fine, i documenti sono spesso corredati da sufficienti informazioni per identificare il soggetto ritratto, mediante indicazione del nome, del link al profilo personale sui social network, dell'indirizzo privato, o del luogo di lavoro. La diffusione produce una significativa lesione della reputazione e della dignità personale dell'interessato. Nei soggetti più deboli ciò potrebbe cagionare danni riflessi all'integrità psicofisica;

[21] per "diffamazione online" si intende la commissione di un fatto discriminatorio nei confronti di qualcuno, mediante l'utilizzo di mezzi di stampa o di pubblicità (art. 595 co.3 c.p.).

[22] La truffa informatica è una fattispecie criminosa sanzionata dall'art. 640-ter c.p. ed introdotta nel nostro ordinamento con la Legge 547 del 1993. Si tratta di un reato che ha due eventi naturalistici, uno di profitto (truffa patrimoniale) e uno di danno (danno al sistema informatico), i quali per consumarsi necessitano di verificarsi entrambi. Si tratta di un reato che quindi va a punire principalmente due condotte, ossia: l'alterazione del funzionamento di un sistema informatico e l'intervento senza diritto su informazioni o programmi informatici. È un reato a forma libera, con dolo generico ed è configurabile il tentativo.

[23] Il furto d'identità digitale è un reato che viene interposto tra la sostituzione di persona e la truffa informatica. Si tratta di un fenomeno che si verifica quando un reo va a trarre in inganno la vittima con lo scopo di sottrarre ad essa le credenziali di un account oppure determinati dati inerenti alla persona nel cyberspazio.

[24] Tra i casi di truffa online più famosi, commessi ai danni dei consumatori, abbiamo i seguenti:

- Pubblicità personalizzata e contenuti scelti per ogni utente.

  Generalmente, alla base del funzionamento della maggior parte dei social, c'è un algoritmo, ossia: "*un programma informatico basato su una sequenza finita di operazioni da svolgere per risolvere un determinato problema* [25]".

  Tale algoritmo, applicato ai social, nella maggior parte dei casi ha la funzione di indicizzare i contenuti per ogni singolo utente, in base alle loro preferenze e alle categorie di video e foto con i quali hanno interagito in precedenza.

  Tale funzione rappresenta naturalmente qualcosa di importante e ad alto tasso di gradimento per molti utenti, poiché permette a questi di poter interagire con contenuti che garantiscono loro una certa soddisfazione.

  Il rischio rappresentato da questa funzionalità è la possibile violazione della privacy degli utenti.

  La possibilità che l'algoritmo, alla base dei social, riesca a memorizzare dati riguardo le nostre preferenze e i nostri gusti personali, rappresenta qualcosa di invasivo e per alcuni intollerabile.

  È importante quindi che venga applicata una giusta regolamentazione all'operato di questi social e anche delle politiche interne accurate, assicurando agli utenti che interagiscono con essi un'esperienza sicura e nel totale rispetto della loro privacy e della loro vita personale.

- il caso PlusToken, ossia un programma di investimenti che proponeva ai suoi utenti guadagni milionari investendo in criptovalute e utilizzando lo schema Ponzi. Inizialmente, come tutti gli schemi Ponzi, i rendimenti erano davvero elevati, ma si basavano sugli introiti derivati dall'arrivo di altri utenti. Quando a giugno 2019 gli amministratori della piattaforma hanno deciso di chiudere il programma, si sono portati via una cifra che aggira intorno a tre miliardi e mezzo di dollari in criptovalute, sparendo nel nulla;
- il caso Onecoin, avvenuto tra il 2014 e il 2017, che interessava una piattaforma di investimenti basata sullo schema Ponzi e promossa dall'imprenditrice bulgara Ruja Ignatova. Secondo le previsioni della Ignatova, in un suo celebre discorso avvenuto alla Wembley Arena nel 2016, la criptovaluta OneCoin avrebbe raggiunto e fatto concorrenza al bitcoin nei successivi due anni. Il risultato di questo programma di investimento è stata una truffa di circa quattro miliardi e mezzo di euro incassati dalla Ignatova, la quale è ancora ricercata con le accuse di frode e riciclaggio di denaro;
- il caso del Fyre Festival, ossia un evento organizzato principalmente tramite Instagram da parte del truffatore Billy McFaraland e sponsorizzato addirittura dalle influencer Bella Hadid e Kendall Jenner. La truffa in questione si basava sull'organizzazione di un finto festival mondiale che avrebbe avuto luogo nel 2017 su un'ipotetica isola delle Bahamas, in realtà inesistente, e che avrebbe coinvolti i più grandi cantanti e dj a livello mondiale. Il risultato è stato che circa cinquemila persone hanno speso tremila dollari a testa per comprare i biglietti di quello che pensavano sarebbe stato l'evento musicale del decennio, ma che in realtà si è rivelato solo un'enorme truffa.

[25] V. Giannotti, Fondamenti di informatica, Università degli studi di Verona, 2016, cap. 2;

- Aumento di opportunità lavorative.

  Grazie ai social e alle piattaforme digitali si è verificato, specialmente nell'ultimo decennio, un aumento esponenziale dei posti di lavoro in tutto il mondo. Basti pensare che già nel 2014, circa il 70% delle ricerche di mansioni o posti lavoro venivano effettuate tramite i social [26].

  Negli Stati Uniti, tra il 2020 e il 2021, sono stati creati circa 17 milioni di nuovi posti di lavoro nel web e nel mondo digitale [27].

  In Italia la situazione è decisamente meno sviluppata, infatti secondo uno studio[28] del Boston Consulting Group, l'Italia è il terzultimo Stato Europeo per quanto riguarda il mercato e l'occupazione dei settori della Digital Economy.

- Dipendenza dai social.

  La dipendenza dai social network, anche conosciuta a livello internazionale come "social media addiction", è un tipo di dipendenza comportamentale caratterizzata da un'eccesiva preoccupazione per l'uso dei social media, accompagnata da un irrefrenabile e incontrollabile bisogno di accedere ad essi.

  Si tratta di una patologia vera e propria che ha raggiunto l'apice di utenti affetti da essa durante gli anni della pandemia.

  Gli individui affetti da questo tipo di dipendenza possono presentare i seguenti sintomi:

  - Tendenza della persona a passare molto tempo sui social a causa di un vero e proprio bisogno o di un'urgenza fisico-psicologica;
  - Incapacità di smettere e astinenza in caso di impossibilità nell'utilizzo di questi strumenti;
  - Continua esigenza dello sharing, ossia: da un lato l'utente sente il bisogno di rimanere aggiornato su tutti i contenuti che vengono postati da parte di persone a cui sono interessate, dall'altro lato invece, l'utente deve

[26] K. Schwab; S. Zahidi, The future of Jobs Report 2020, World Economic Forum, 2020;

[27] Vedi nota precedente;

[28] Boston Consulting Group, Sizing the digital economy, 2020; il BCG, ossia il Boston Consulting Group è una multinazionale di consulenza strategica di alta direzione, leader nel panorama mondiale, che da oltre cinquant'anni assiste il management delle aziende di ogni settore nell'identificare, e realizzare insieme, fattori di vantaggio competitivo sostanziali, concreti e duraturi.

necessariamente condividere foto, video o informazioni varie riguardo la propria vita, con lo scopo di tenere gli altri aggiornati a riguardo;

- Peggioramento dell'umore e problemi socio-relazionali.

Quindi, in conclusione, sono stati analizzati i vari rischi e benefici che possono derivare dall'utilizzo dei social network e delle piattaforme digitali.
Il mondo virtuale e l'iper-connessione in cui viviamo oggi, sono effettivamente sia uno strumento che un rischio, in quanto capaci di garantire enormi vantaggi e soluzioni per chi ne sappia sfruttare il potenziale, ma allo stesso tempo in grado di provocare pericoli e rischi non poco rilevanti.
Ciò che sarà interessante è analizzare quale siano la responsabilità e il ruolo dell'I.S.P. nella regolamentazione e nella gestione del traffico in queste piattaforme, verificando come quest'ultimo possa interagire per limitare al massimo qualsiasi rischio o pericolo, garantendo così un ambiente digitale più sicuro per chi lo utilizza.

PARTE II

2) Responsabilità dell'Internet Service Provider.

Nel presente capitolo si vuole analizzare quello che è effettivamente il cuore di questo elaborato, ossia: "*la Responsabilità dell'I.S.P.*".

Si partirà prima di tutto da un'indagine del quadro normativo Europeo e Nazionale, passando poi ad un'analisi dettagliata dei ruoli e delle posizioni che possono essere ricoperti dal Provider, arrivando infine come conclusione all'illustrazione di alcuni casi pratici di Giurisprudenza che hanno avuto un ruolo cruciale per lo sviluppo della tematica in questione.

Lo scopo del capitolo in esame è quello di evidenziare come la responsabilità del Provider si sia evoluta nel corso de tempo e quanto spesso l'I.S.P. sia stato messo sotto giudizio per questioni di responsabilità omissiva e commissiva, con riferimento ad alcune vicende che hanno interessato direttamente la piattaforma digitale o il sistema da essi gestiti.

Molte sono le sfaccettature quando si parla del ruolo e della responsabilità Provider e, molti sono gli scenari che ne possono derivare, ciò che è importante è soffermarsi su come la responsabilità del Provider è stata interpretata fino ad oggi nei vari casi pratici che si sono susseguiti nel nostro ordinamento, ma anche a livello Europeo.

2.1.) Direttiva n. 31/2000: "E-commerce".

La Direttiva E-commerce è frutto di un progetto normativo iniziato nel 1998 e portato a termine nel 2000, anno in cui è stata definitivamente approvata ed entrata in vigore.

La Direttiva in questione nasce con l'obiettivo di garantire, tutelare e consentire lo sviluppo dei servizi, tra gli Stati Membri dell'UE, in quella che viene definita come "*la società dell'informazione* [29]", ossia un contesto in cui le nuove tecnologie informatiche e di telecomunicazione assumono un ruolo fondamentale nello sviluppo delle attività umane.

Precedentemente all'avvento della Direttiva esistevano due tesi, completamente contrapposte tra loro [30], le quali si scontravano nel fornire una definizione effettiva di cosa si intendesse quando si faceva riferimento all'E-commerce; queste tesi erano le seguenti:

[29] Avv. A. Calia; "Diritto e tecnologie digitali, quali vantaggi e quali rischi?", Università degli studi di Cagliari, 2019, pag. 7;

[30] Avv. P. Severino: "controlli e controllori. Nuovi diritti e posizioni di garanzia nel cyberspazio", Libera Università degli studi sociali Guido Carli, 2022.

a) *tesi espansiva, secondo la quale l'e-commerce viene inteso come: "una serie di transazioni commerciali che includono sia gli organizzatori che i singoli individui, transazioni che sono basate nel processare e trasmettere dati digitali di varie tipologie";*

b) *Tesi restrittiva, secondo la quale invece si faceva riferimento solamente alle transazioni commerciali che avvenivano attraverso l'utilizzo di internet*.

Con l'avvento della Direttiva E-commerce si cerca di ristabilire ordine ai dibattiti avvenuti in precedenza per quanto riguarda la definizione di E-commerce.
Prima di tutto la Direttiva riporta alcune differenziazioni, quali:

- la prima che va a separare la figura del "*commercio elettronico diretto* [31]", inteso come pagamenti ed esecuzioni di prestazioni online, da quella del "*commercio elettronico indiretto*", considerato invece come quel genere di commercio in cui, se si tratta di un bene materiale, allora la consegna di questo avverrà con metodi tradizionali.

  Quando si fa riferimento al termine "*commercio elettronico diretto*" è imperativo aggiungere una definizione di cosa si intenda per "*servizio a distanza*", definizione che non è stata facilmente comprensibile poiché in origine non si era certi di cosa si intendesse con questo termine, sé un servizio fornito per via elettronica/telematica e quindi con totale assenza fisica delle parti, o sé un servizio ricevuto e inviato con l'ausilio di mezzi elettronici, a richiesta individuale di un destinatario del servizio.
- tornando ora alla definizione di E-commerce, la seconda differenziazione fa capo precisamente a quattro aspetti dell'interazione, ossia:
  a) Business to consumer: consumatori che vengono considerati come utenti finali [32];
  b) Business to business: consumatori intesi come aziende e/o professionisti;
  c) Consumer to consumer: che fa riferimento invece a quelle transazioni realizzate direttamente tra i privati;

[31] Art. 2 Dir. n. 98/34/CE, modificata dalla Dir. 98/48/CE
[32] Cfr. G. De Nova, F. Delfini, La direttiva sul commercio elettronico: prime considerazioni, in «Rivista di diritto privato», 2000, vol. 2, fascicolo 4, pp. 693-704.

d) Business to administration: quelle transazioni che avvengono tra Pubblica Amministrazione e imprese/cittadini

Secondo quanto espresso dalla Commissione Europea nella Com. n. 97/157, il commercio elettronico può essere definito come[33]: "*un commercio che consiste nello svolgimento delle attività commerciali per via elettronica. Si tratta di un commercio basato sull'elaborazione e la trasmissione dei dati per via elettronica, andando a comprendere tutte le varie attività di commercializzazione di merci e servizi per via elettronica, distribuzione online di contenuti digitali, effettuazioni per via elettronica di operazioni di trasferimento fondi […]*"

La normativa vigente, partendo dall'art.1, ci dice quanto segue: "*la presente direttiva mira a contribuire al buon funzionamento del mercato garantendo la libera circolazione dei servizi della società dell'informazione tra gli stati membri* [34]".

A primo impatto, se si va a paragonare la normativa in questione con l'attuazione che viene data all'art. 1 co.1 del D.lgs. n.70/2003 [35] , si può notare sin da subito un certa discordanza tra le due, dovuta al seguente motivo: : nella Direttiva 31/2000, precisamente nell'art.1 co.1, si nota come l'obbiettivo principale sia quello di conseguire un "*buon finanziamento del mercato*"; nell'art. 1 co.1 del D.lgs. n. 70/2003 si afferma invece che, tra gli obiettivi che il legislatore si prefigge, vi è quello di "*promuovere la libera circolazione dei servizi della società dell'informazione, fra i quali il commercio elettronico*."

Spostandoci poi sull'articolo seguente, ossia l'art. 2, vediamo come questo sia inteso a dare delle definizioni esplicative di alcune terminologie generali, quali ad es:

- *prestatore*, ossia la persona fisica o giuridica che presta un servizio della società dell'informazione
- *Destinatario del servizio*, ossia la persona fisica o giuridica che, a scopi professionali e non, utilizza un servizio della società dell'informazione, in particolare per ricercare o rendere accessibili delle informazioni;

[…]

[33] Commissione Europea, Com. n. 97/157

[34] Art. 1 par. 1 Dir. n. 31/2000, "obiettivi e campo di applicazione".

[35] Art. 1 co.1 D.lgs. 70/2003: "Il presente decreto è diretto a promuovere la libera circolazione dei servizi della società dell'informazione, fra i quali il commercio elettronico".

Una definizione, riportata sempre nell'art. 2, che deve essere necessariamente menzionata è quella di: "*comunicazioni commerciali*", considerate come "*tutte le forme di comunicazione destinate, in modo diretto o indiretto, a promuovere beni, servizi o l'immagine di un'impresa, di un'organizzazione o di una persona che esercita un'attività commerciale, industriale, artigianale o una libera professione* [36]".

Basandoci su quanto espresso dall'art. 2, non rientrano nella definizione di "comunicazioni commerciali [37]" le seguenti:

- *indicazioni necessarie per accedere direttamente all'attività di tale impresa, organizzazione o persona, come un nome di dominio (domain name) o un indirizzo di posta elettronica;*
- *le comunicazioni relative a beni, servizi o all'immagine di tale impresa, organizzazione o persona elaborate indipendentemente da essa, in particolare se a titolo gratuito.*

Di rilevante importanza, sempre con riferimento all'argomento delle comunicazioni commerciali, è la figura del prestatore [38], un soggetto che ha il ruolo di rendere accessibili e consultabili alcune informazioni, anche quando non si perviene alla conclusione di un contratto con il cliente [39], quali ad es: il nome, l'indirizzo geografico, dati di consultazione e gli estremi del registro commerciale o dell'indirizzo professionale.

Secondo quanto previsto dalla Normativa E-commerce: "*gli stati membri devono provvedere affinché le comunicazioni commerciali costituenti un servizio della società dell'informazione, o parte integrante di esso, rispettino i seguenti requisiti minimi [40]:*

- *la comunicazione commerciale deve essere facilmente distinguibile e identificabile come tale;*
- *la persona fisica o giuridica per conto della quale viene effettuata la comunicazione commerciale;*
- *le offerte promozionali, come ribassi, premi od omaggi, qualora permesse dallo Stato membro in cui è stabilito il prestatore, devono essere chiaramente*

[36] Art. 2 lett. F, Dir. n. 31/2000
[37] Art. 2 lett F, Dir. 31/2000
[38] Art. 2 lett. B, Dir. n. 31/2000, si veda la definizione riportata in questa pagina
[39] Art. 5 Dir. n. 31/2000: "informazioni generali da fornire"
[40] Art. 6 Dir. 31/2000: "informazioni da fornire"

identificabili come tali; le condizioni per beneficiarne devono essere facilmente accessibili e presentate in modo chiaro e inequivocabile;

- *i concorsi o giochi promozionali, qualora siano permessi dallo Stato membro in cui è stabilito il prestatore, devono essere chiaramente identificabili come tali; le condizioni di partecipazione devono essere facilmente accessibili e presentate in modo chiaro ed inequivocabile*".

È possibile affermare che, attraverso la Direttiva E-commerce, si abbandona la definizione di commercio elettronico e si arriva a quella di "servizi della società dell'informazione", ossia: "*quei servizi prestati dietro retribuzione, a distanza per via elettronica, mediante apparecchiature elettroniche di elaborazione e di memorizzazione di dati, a richiesta di un destinatario del servizio* [41]".

Tutto ciò ha spianato la strada per la nascita della c.d. *"dot.com",* ossia delle imprese virtuali, che operano nella rete, ma che naturalmente possono avere anche una sede fisica, come ad esempio Facebook e Hotmail.

Tutto questo è incentrato principalmente su un unico obiettivo, ossia quello di rimuovere le barriere nazionali alle transazioni che si svolgono online, così da garantire una maggiore unione e connessione tra gli stati membri.

Questo ha portato anche alla nascita, nel 2010, "dell'*Agenda Digitale Europea* [42]", un'iniziativa chiave volta a regolamentare e promuovere l'utilizzo delle tecnologie dell'informazione e della comunicazione, a creare condizioni di parità sui mercati digitali con le grandi piattaforme, e a rafforzare la sovranità digitale dell'UE, durante il biennio 2020-2030. L'ostacolo maggiore, al raggiungimento dell'obbiettivo di rimozione delle barriere nazionali, è rappresentato naturalmente dalla grande divergenza normativa che c'è tra i singoli stati membri dell'UE, alla quale segue anche un enorme difficoltà nell'individuare la disciplina applicabile.

[41] Art 4. Par. 25 GDPR, che rinvia all'Art. 1 par. 1 lett. b) della Dir. 2015/1535

[42] l'Agenda Digitale Europea del biennio 20-30 è il successore della precedente Agenda Digitale, nata nel biennio 10-20. Mentre la "vecchia" Agenda era finalizzata a migliorare l'accesso ai beni e servizi digitali per i consumatori e le imprese in tutta Europa dotando l'UE di un sistema avanzato in materia di diritti degli utenti e protezione dei consumatori e delle imprese, la "nuova" è incentrata sui profondi cambiamenti introdotti dalle tecnologie digitali, sul ruolo essenziale svolto dai servizi e dai mercati digitali e sulle nuove ambizioni dell'UE in campo tecnologico e geopolitico.

L'opzione di fondo della disciplina della libera prestazione dei servizi della società dell'informazione è costituita dalla c.d. "*clausola del mercato interno*[43]", che conferisce ai prestatori di servizi *on line* il diritto di operare in tutta l'UE, restando soggetti alle norme del paese d'origine.

Tale clausola fa riferimento al c.d. "criterio dello stabilimento", definito come esercizio effettivo di una attività economica, per una durata di tempo indeterminata mediante insediamento in pianta stabile, che esclude quindi il collegamento con il luogo in cui si trova la tecnologia di supporto del sito.

Il criterio dello stabilimento è, dunque, principio rilevante ai fini dell'individuazione della legge da applicare.

La Direttiva n.31/2000 ha un ambito di applicazione alquanto vasto che non si limita soltanto alle attività dei servizi della società dell'informazione, ma che si estende anche alla regolamentazione dell'attività del provider, di cui agli artt. 14,15,16 e 17, come vedremo nei paragrafi successivi.

Gli unici servizi che non rientrano nell'area di competenza della Direttiva sono i seguenti:

- le questioni supplementari di diritto internazionale privato;
- Le questioni riguardanti i servizi di prestatori stabiliti in un paese terzo;
- I settori tributati, le attività di notai o di altre professioni equivalenti se queste abbiano un nesso diretto e specifico con l'esercizio di pubblici poteri, giochi d'azzardo e la rappresentanza/difesa processuale;
- Le questioni relative ai servizi della società dell'informazione oggetto delle Direttive 95/46/CE e 97/66/CE;
- La materia fiscale e, segnatamente, l'IVA, la quale va a interessare numerosi servizi contemplati dalla Direttiva e-commerce[44].

[43] S. Saracco: "il fenomeno dell'E-commerce e i recenti sviluppi del mercato unico digitale in Europa", Giureta 2016, vol. XIV, pag. 94.

[44] C. Rossello, La nuova disciplina del commercio elettronico. Principi generali ed ambito di applicazione, in Commercio elettronico, documento informatico e firma digitale. La nuova disciplina, Torino, 2003, pag.16.

2.2) D.lgs. 70/2003, "Codice del Commercio Elettronico".

Il Decreto in questione rappresenta la normativa mediante la quale la Direttiva n. 31/2000 è stata ratificata dal nostro Paese e applicata al nostro ordinamento.

L'approvazione di tale Decreto è finalizzata al perseguimento di due principali obbiettivi, i seguenti:

- fornire una regolamentazione nazionale uniforme alla materia del commercio elettronico, sempre facendo capo agli standard forniti dall'Unione Europea;
- Dare applicazione alla c.d. "*clausola del mercato interno*[45]", la quale è finalizzata principalmente ad assicurare la libera prestazione dei servizi online all'interno della Comunità Europea.

Come si è detto, sin dal primo articolo, l'attuazione italiana sembra il frutto di un'opera di diversificazione, sotto taluni aspetti.

La normativa Europea tende a focalizzarsi principalmente sul buon finanziamento del marcato interno, per poi dedicarsi alla promozione dei servizi della società dell'informazione; allo stesso tempo la normativa italiana mette i servizi della società dell'informazione subito in primo piano.

La differenziazione qui sopra riportata ci serve a comprendere al meglio quali sono le esigenze che il nostro Paese ha ritenuto porre al primo piano rispetto a quelle menzionate dall'Unione Europea.

Prima di passare ad un'analisi più interna e strutturale del D. lgs. 70/2003, è necessario ripercorrere storicamente tutte le precedenti normative che hanno regolamentato il settore dell'E-commerce nel nostro ordinamento.

Prima della normativa in esame, ci sono state due altre normative principali che hanno caratterizzato la regolamentazione del settore dell'E-commerce nel nostro ordinamento, ma anche a livello Europeo, ossia:

1. Il D. lgs. 31 marzo 1998, n. 114, anche conosciuto come il "Decreto Legislativo Bersani", il quale racchiude in sé la riforma della disciplina dell'esercizio delle

[45] La clausola relativa al mercato interno è un principio fondamentale della direttiva sul commercio elettronico. Garantisce che i prestatori di servizi online siano soggetti al diritto dello Stato membro in cui sono stabiliti e non al diritto degli Stati membri in cui il servizio è accessibile; https://digital-strategy.ec.europa.eu/it/policies/e-commerce-directive#:~:text=La%20clausola%20relativa%20al%20mercato%20interno%20è%20un%20principio%20fondamentale,cui%20il%20servizio%20è%20accessibile.

attività commerciali. La peculiarità di questa normativa, è che qui il commercio elettronico non trova uno spazio autonomo nel quale viene menzionato, anzi, esso viene solamente relegato all'art. 4 co.1, nel quale si tratta delle "forme speciali di vendita al dettaglio", con riferimento alla vendita per corrispondenza o tramite televisione o altri sistemi di comunicazione.

La normativa offre un quadro esplicativo di quali sono gli obblighi e le tempistiche che si devono rispettare nel caso in cui un soggetto abbia intenzione di avviare un'attività commerciale, come ad es. gli obblighi di comunicazioni, le loro caratteristiche e le sanzioni in caso di omissioni o inosservanze di tempistiche e regole.

2. Il D. lgs. 22 maggio 1999, n. 185, redatto in seguito all'enorme crescita ed espansione del fenomeno di internet. Si tratta della normativa mediante la quale è stata ratificata la Dir. n. 97/7/CE [46], una Direttiva comunitaria mediante la quale si cerca di creare un quadro generale per la protezione dei consumatori in materia di contratti a distanza. Mediante tale strategia si è cercato di creare una disciplina uniforme, nell'ambito delle tutele, in relazione dei contratti stipulati dai consumatori dei diversi Stati Membri.

Il D.lgs. 70/2003 è una normativa composta da 22 articoli, la quale non si limita solo alla regolamentazione del Commercio Elettronico nel nostro ordinamento, ma anzi si occupa di fornire anche un quadro di regole e norme che hanno lo scopo di disciplinare la figura del Prestatore di servizi della Società dell'informazione, conosciuto appunto come Internet Service Provider.

I principali articoli della normativa in questione sono i seguenti:

- L' art. 1, mediante il quale si vanno ad evidenziare quelle che sono le finalità che si intendono perseguire, ossia:
    a) i rapporti fra contribuente e amministrazione finanziaria connessi con l'applicazione, anche tramite concessionari, delle disposizioni in materia di tributi nonché la regolamentazione degli aspetti tributari dei

[46] È grazie a questa Direttiva 97/7/CE che si ha per la prima volta la definizione di "contratto a distanza", inteso come: "qualunque contratto avente per oggetto beni o servizi che impieghi esclusivamente una o più tecniche di comunicazione a distanza fino alla conclusione del contratto."

servizi della società dell'informazione ed in particolare del commercio elettronico;

b) le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni di cui alla legge 31 dicembre 1996, n. 675, e al decreto legislativo 13 maggio 1998, n. 171, e successive modificazioni;
c) Le intese restrittive della concorrenza;
d) Le prestazioni di servizi della società dell'informazione effettuate da soggetti stabiliti in Paesi non appartenenti allo spazio economico europeo;
e) le attività, dei notai o di altre professioni, nella misura in cui implicano un nesso diretto e specifico con l'esercizio dei pubblici poteri;
f) La rappresentanza e la difesa processuali;
g) i giochi d'azzardo, ove ammessi, che implicano una posta pecuniaria, i giochi di fortuna, compresi il lotto, le lotterie, le scommesse i concorsi pronostici e gli altri giochi come definiti dalla normativa vigente, nonché quelli nei quali l'elemento aleatorio è prevalente.

- nell'art. 2 invece è presente un quadro di definizioni alquanto ampio, che include quelle di prestatore del servizio, servizi della società dell'informazione, destinatario del servizio e molte altre;[47]
- L'art. 3 è dedicato alla regolamentazione del mercato interno, con tutte le deroghe che verranno poi menzionate negli articoli seguenti;
- l'art. 7, il quale tratta delle "*informazioni generali obbligatorie*" (già trattate anche in precedenza con la Direttiva n. 31/2000) che devono essere fornite dal prestatore nei confronti del destinatario del servizio o delle Autorità, informazioni

[47] L'ambito regolamentato, secondo l'art.2 lett. H è il seguente: L'ambito regolamentato riguarda le disposizioni che il prestatore deve soddisfare per quanto concerne:

1. l'accesso all'attività di servizi della società dell'informazione, quali le disposizioni riguardanti le qualifiche e i regimi di autorizzazione o di notifica;
2. l'esercizio dell'attività di un servizio della società dell'informazione, quali, ad esempio, le disposizioni riguardanti il comportamento del prestatore, la qualità o i contenuti del servizio, comprese le disposizioni applicabili alla pubblicità e ai contratti, ovvero alla responsabilità del prestatore.

come ad es: il nome, la denominazione sociale, il domicilio o la sede legale, le professioni regolamentate, i vari prezzi e tariffe dei servizi […]

- L'art. 8, il quale dispone quali siano gli obblighi di informazione per le comunicazioni commerciali. In base a quanto stabilito dall'articolo in questione: "le comunicazioni commerciali, sin dal loro primo invio, devono contenere in modo chiaro e inequivocabile, una specifica informativa, diretta ad evidenziare:
    a) che si tratta di comunicazione commerciale;
    b) La persona fisica o giuridica per conto della quale è effettuata la comunicazione commerciale;
    c) Che si tratta di un'offerta promozionale come sconti, premi o omaggi e le relative condizioni di accesso;
    d) Che si tratta di concorsi o giochi promozionali, se consentiti, e le relative condizioni di partecipazione".

- L'art. 12, il quale tratta della materia inerente alla conclusione del contratto, un argomento alquanto interessante e che deve essere necessariamente trattato.
  Nel co.1 si stabilisce quanto segue: "oltre agli obblighi previsti dalla legge, il prestatore di un servizio della società dell'informazione, salvo diversi accordi, deve fornire le seguenti informazioni:
    a) le varie fasi tecniche da seguire per la conclusione del contratto;
    b) il modo in cui il contratto concluso sarà archiviato e le relative modalità di accesso;
    c) i mezzi tecnici messi a disposizione del destinatario per individuare e correggere gli errori di inserimento dei dati prima di inoltrare l'ordine al prestatore;
    d) gli eventuali codici di condotta cui aderisce e come accedervi per via telematica;
    e) le lingue a disposizione per concludere il contratto oltre all'italiano;
    f) l'indicazione degli strumenti di composizione delle controversie.

> Il comma 1 dell'art.12 non è applicabile ai contratti conclusi esclusivamente mediante scambio di messaggi di posta elettronica o comunicazioni individuali equivalenti.

La normativa in questione stabilisce inoltre all'art. 6 che: "*l'accesso all'attività di un prestatore di un servizio della società dell'informazione e il suo esercizio non sono soggetti, in quanto tali, ad autorizzazione preventiva o ad altra misura di effetto equivalente* [48]".

2.2.1) attività dell'Internet Service Provider

La normativa vigente, come detto anche in precedenza, si occupa anche della regolamentazione dell'I.S.P., con riferimento principalmente all'attività da questi svolta e alle sue responsabilità.

Il provider, anche conosciuto come prestatore intermediario, è: "*quel soggetto che esercita un'attività imprenditoriale che offre agli utenti la fornitura di servizi inerenti internet, in sostanza è colui che fornisce ai terzi l'accesso alla rete, utilizzando una connessione remota tramite linea telefonica o banda larga* [49]".

L'I.S.P. dunque è quel soggetto che presta dei servizi fondamentali per il funzionamento della rete e garantisce agli utenti una connessione ad internet.

Il provider, per garantire questo accesso ad internet, instaura dei rapporti con i seguenti soggetti:

a) il gestore della rete di telecomunicazione;
b) il network information service, che in Italia vede la sua rappresentanza nel Gruppo di Armonizzazione Reti e Ricerca del Consiglio Nazionale.

Per garantire il collegamento dell'utente alla rete, il prestatore assegna al computer del soggetto in questione un indirizzo IP (Internet Protocol), ossia un codice identificativo che consente di identificare la nostra presenza sulla rete pubblica del web.

[48] Art. 6 D.lgs. 70/2003

[49] M.Iaselli, "Internet Service Provider, guida all'ISP: cos'è, tipologie e regimi di responsabilità", Wolters Kluwer, Altalex, 2019;

Gli indirizzi IP possono essere di varie categorie, una prima distinzione deve essere fatta tra IP pubblico e IP privato:

- IP pubblico, anche inteso come esterno, ossia un codice identificativo univoco che l'I.S.P. assegna ad ogni utente appartenente alla sua rete. Tale categoria di indirizzo IP viene utilizzata con lo scopo di identificare la rete domestica in internet e permettere ad es. la comunicazione tra due computer non appartenenti alla stessa LAN (local area network [50]);
- IP privato, ossia quello utilizzato per identificare i dispositivi di rete appartenenti ad una stessa LAN. L'assegnazione degli indirizzi IP è deputata al router e può avvenire in maniera o automatica o manuale, sempre ad opera del gestore locale. Ciò permette di identificare univocamente ogni dispositivo di rete all'interno di una rete locale, ma non al suo esterno.

Una seconda distinzione deve essere fatta invece tra IP statico, dinamico e "nattato", come segue:

- Statico, si tratta di un tipo di indirizzo IP che si distingue da quello dinamico per via degli elevati costi richiesti per la sua installazione e utilizzo (viene infatti utilizzato solitamente da imprese di medio-grandi dimensioni);
- Dinamico, si tratta di una categoria di indirizzi IP più facilmente accessibile per via della sua economicità (viene utilizzato principalmente per utenza domestica). Si tratta di un indirizzo IP tra i più diffusi, vista la sua capacità di soddisfare maggiormente le ordinarie esigenze degli utilizzatori;
- Nattato, con questo termine facciamo riferimento ad un IP che utilizza la tecnologia NAT, ossia: "network access translation", una tecnologia che permette di gestire gli indirizzi IP di una rete locale LAN in modo da garantire la comunicazione con altre reti, siano esse domestiche o internet.

[50] La LAN, anche nota come rete locale, nasce come progetto ideato dalla Olivetti s.p.a. tra la fine del 1970 e primi anni del 1980 ed utilizzata per la prima volta come un prototipo per il sistema di votazione elettronica del parlamento. La LAN può essere definita come una rete informatica estendibile ad un'area geografica limitata come una casa o una scuola. La LAN non deve essere confusa con la WAN (wide area network) visto che quest'ultima presenta un'estensione una portata molto più elevata, garantendo la possibilità di mettere in connessione utenti appartenenti ad aree geografiche molto distanti tra loro.

Ci sono poi alcuni altri aspetti che avrebbero bisogno di una trattazione più accurata, come ad esempio l'utilizzo dei server proxy, anche conosciuti come virtual private network, ma nell'elaborato in questione ci si limiterà solamente ad un'analisi più generale degli Indirizzi IP, evitando di cadere troppo nei dettagli tecnici.
Quindi, in pratica, quando un determinato utente, in possesso di un certo indirizzo IP, effettua una ricerca o richiesta attraverso il web, questa richiesta verrà inoltrata all'ISP, il quale sarà al corrente di ciò che è stato domandato.
Nel caso in cui venga commesso un attacco informatico da un utente che è identificato sotto un determinato indirizzo che appartiene a un gestore specifico, la polizia potrà recarsi dal gestore in questione è richiedere informazioni a riguardo [51].
Tornando ora alle attività svolte dall'I.S.P. si può vedere come queste vengano disciplinate dal D.lgs. 70/2003, rispettivamente nei seguenti articoli:

- Art. 14: "*attività di accessing".* Anche conosciuta come "*mere conduit",* si tratta dell'attività in cui il provider va semplicemente a svolgere quella che è l'attività di trasporto dei dati, fornendo quindi un'attività di connessione/trasmissione. In base a quanto stabilito dalla normativa in questione, l'access provider è quella figura che si occupa o di trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o di fornire un accesso alla rete di comunicazione. L'access provider è quindi quello che si interessa di meno delle informazioni che vengono trasmesse, poiché appunto egli ha il solo compito di trasportarle, e non è responsabile di queste informazioni a condizione che:

1. Non dia origine alla trasmissione;
2. Non selezioni il destinatario della trasmissione;
3. Non selezioni né modifichi le informazioni trasmesse.

Condizione preliminare e necessaria per questa attività, da parte degli utenti, è la possibilità di essere connessi a internet. L'accesso a internet viene ottenuto generalmente

[51] In questo caso vengono messe in atto le c.d. "indagini informatiche", indagini portate avanti dalle autorità con lo scopo di estrarre o cercare tracce informatiche.
Con tali indagini si cerca quindi di ricostruire, in un ambiente digitale, il comportamento umano considerato criminoso, attraverso l'utilizzo di indicatori digitali e non fisici.
Le indagini informatiche possono svolgersi o materialmente, quando si ha la disponibilità materiale del dispositivo che contiene le tracce, o da remoto, quando invece non si hanno tracce fisiche.

stipulando un contratto specifico con un internet access provider, il quale provvederà a fornire la password e il nome utente, necessari per accedere al servizio fornito, all'abbonato.

- Art. 15: *"attività di caching"*. In questo caso non si fa più riferimento all'access provider bensì al "caching provider", ossia colui che agisce con lo scopo di memorizzare temporaneamente i dati, con il secondo fine di rendere più efficace il successivo inoltro ad altri destinatari, sotto loro richiesta.

  Secondo quanto espresso dall'art. 15, si devono rispettare le seguenti condizioni:

1. *le informazioni non devono essere modificate;*
2. *Si devono rispettare le condizioni di accesso alle informazioni;*
3. *Tale attività si deve conformare alle norme di aggiornamento delle informazioni, indicate dalle imprese del settore;*
4. *Non si deve interferire con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore, per ottenere dati sull'impiego delle informazioni;*
5. *Si deve agire prontamente con lo scopo di rimuovere le informazioni che ha memorizzato o per disabilitarne l'accesso*;

- A*rt. 16: "attività di hosting"*. Si tratta dell'attività più importante tra le tre e di quelle che maggiormente si è trovata al centro di dibattiti e discussioni nel corso degli anni [52]. In questo caso l'I.S.P. assume la veste dell'Hosting Provider, una figura che ha il ruolo di svolgere una memorizzazione stabile dei dati forniti da un destinatario del servizio, vale a dire quindi che si occupa dell'archiviazione dei dati in transito al fine di renderli reperibili.

  L'hosting provider può essere quindi definito come un prestatore che svolge dei servizi di memorizzazione su richiesta di un destinatario del servizio, oppure come il tramite che fornisce a professionisti, aziende e individui la tecnologia necessaria per far si che i propri siti e pagine web siano visibili su internet.

  L'hosting provider non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore rispetti le seguenti condizioni:

1. Non sia effettivamente a conoscenza del fatto illecito;

[52] Vedere capitolo 1

2. Non appena a conoscenza dei fatti, su comunicazione delle autorità, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

La figura del Provider che fornisce servizi di hosting è stata per molto tempo, ed è ancora oggi, oggetto di critiche e discussioni, sia in Dottrina che in Giurisprudenza. Sono sorti molti dubbi riguardo la figura in questione e la sua effettiva responsabilità, primo fra tutti quello che fa riferimento a quando l'hosting provider possa essere considerato come effettivamente a conoscenza della fattispecie criminosa.

2.2.2) hosting provider attivo e passivo, art. 17 D.lgs. 70/2003.

Il tema fondamentale che si intende esplorare e comprendere a fondo, quando si parla del ruolo e della responsabilità del Provider (hosting in questo caso), è quello che riguarda l'imputabilità dei soggetti che gestiscono servizi di hosting e di connessione riguardo la commissione di un illecito, da parte di terzi, sulle loro piattaforme.
Si tratta di un tema assai complicato, soggetto a molte dispute in Giurisprudenza e in Dottrina, vista la presenza di esigenze che richiedono l'assenza di limiti e censure nella navigazione in internet, e bisogni di far diventare la rete un luogo sicuro, imponendo così restrizioni e limiti.
Con riferimento a questa tematica si sono andate a contrapporre con il tempo tre tesi, le seguenti [53]:

a) *internet senza obblighi di censura: i sostenitori di questa tesi ritengono che il legislatore dovrebbe astenersi dal dettare regole ad hoc per prevenire la commissione di reati su internet. Normalmente questo non concede la possibilità a ciascuno di agire al di fuori dei limiti imposti dall'ordinamento, ma soltanto che, in caso di commissione di un illecito via web, non giustifichi la possibilità di adottare meccanismi di censura preventiva;*
b) *Internet con obblighi di censura e di controllo: secondo tale tesi, la rete deve essere considerata come un fattore di rischio per la garanzia dei diritti, rispetto al quale il legislatore non può mostrarsi indifferente. Quindi lo scopo di questa*

[53] A. Ingrassia: "il ruolo dell'ISP nel cyberspazio: cittadino, controllore o tutore dell'ordine?", 2010, par. 1.2, pagg. 5 e 6;

argomentazione è prevenire che si arrivi alla lesione o all'esposizione al pericolo del bene giuridico tutelato;

c) *Responsabilità limitata del provider: secondo tale punto di vista, il provider deve attivarsi a determinate condizioni. Si tratta della tesi prevalente e maggiormente supportata nel nostro ordinamento. I sostenitori di questa tesi affermano che l'internet deve essere, in certi casi, sottoposto al controllo.* L'argomentazione che si vuole illustrare attraverso il punto c) è l'assenza della necessità di esigere un controllo a tappeto sulla rete, promuovendo più che altro dei controlli *necessari al caso che si prende in esame.*

In base a quanto stabilito dalla normativa vigente, il Provider ha l'obbligo di collaborare con le autorità quando si fa riferimento a contenuti illeciti. Questo obbligo si può sostanziare in una serie di ordini di rimozione di contenuti illeciti, la cui violazione determina la responsabilità dell'I.S.P.

Per comprendere a fondo tali meccanismi è necessario esaminare il disposto dell'art. 17 D.lgs. 70/2003, intitolato: "*assenza dell'obbligo generale di sorveglianza*"; tale normativa esprime ciò che segue: "*Nella prestazione dei servizi indicati negli artt. 14, 15, 16, il prestatore non è soggetto a un obbligo generale di controllo e sorveglianza sulle informazioni che va a trasmettere e memorizzare; quindi si parla di un'irresponsabilità del provider e si smentisce l'esistenza di un obbligo giuridico di garanzia*".

Il co. 2 dell'art. 17 precisa che:

a) "*il provider dovrà fornire comunque delle informazioni alle autorità giudiziarie/amministrative aventi funzioni di vigilanza, in caso di entrata a conoscenza con delle presunte attività o informazioni considerate come illecite e riguardanti un suo destinatario del servizio della società dell'informazione;*

b) *Dovrà inoltre procedere senza indugio a fornire alle autorità competenti, su richiesta di queste, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite*".

Le posizioni che possono essere assunte dal Provider sono molteplici; secondo quanto sostenuto dalla Dottrina [54] ci possono essere tre tesi opposte tra loro quando si parla del ruolo del Provider, ossia:

1. *Provider come comune cittadino, figura che viene messa sullo stesso livello di tutti gli altri utenti. In base a tale impostazione, il Provider risponde solamente in caso di commissione da parte sua di un illecito, o nel caso di aiuto fornito ad un reo nella commissione della fattispecie criminosa;*
2. *Provider come controllore del cyberspazio, secondo la quale il Provider viene posto al vertice del controllo sul cyberspazio e assume quindi la posizione di una figura che agisce come una vera e propria autorità di vigilanza[55];*
3. *Provider come tutore dell'ordine, dove invece il Provider viene visto come un vero e proprio ausiliario delle autorità, il quale agisce per coadiuvare l'operato di queste.*

A riguardo occorre distinguere i due ruoli che il Provider può assumere, ossia quelli di I.S.P. Attivo e I.S.P. Passivo.

Partendo da quello attivo, secondo la definizione fornita dalla Suprema Corte di Cassazione [56], si tratta di una posizione ricoperta dal Provider quando quest'ultimo: "*svolge un'attività che esula da un servizio di ordine meramente tecnico, automatico e passivo, e realizza invece una condotta attiva*". Quindi il Provider attivo può essere definito come quel provider che adotta una condotta di azione che completa o arricchisce, in modo non passivo, la fruizione dei contenuti. Attraverso questa massima, la Suprema Corte di Cassazione tende a descrivere il Provider come un soggetto che si interessa dei contenuti da esso veicolati che vi interagisce in modo da arricchirne la loro fruizione da parte degli utenti.

Tale attività può essere desunta da una serie di indici di interferenza che devono essere accertati dal Giudice, quali ad es. l'attività di filtro, di indicizzazione, di organizzazione,

[54] A. Ingrassia: "il ruolo dell'ISP nel cyberspazio: cittadino, controllore o tutore dell'ordine?", 2010, par. 1.2, pag. 6.

[55] Si tratta di una tesi che è stata totalmente scartata dalla Dottrina e dalla Giurisprudenza, poiché considerata non coincidente con il dettato normativo, in quanto non si poteva andare a ritenere la figura del provider come un controllore al pari delle autorità competenti.

[56] Cass. Civ. Sent. n. 7708/2019;

d'uso, di modifica, tutte attività che vengono operate mediante una gestione imprenditoriale del servizio.
Si tratta, quindi, di una figura che viene coinvolta attivamente nella gestione e nella manutenzione dei server e dei contenuti ospitati, in quanto un'attenzione ai contenuti è importante per mantenere la qualità del servizio e l'esperienza dell'utente.

Quando facciamo riferimento alla definizione e delimitazione dei servizi aggiuntivi, i quali vanno appunto a mutare la natura del Provider da passivo ad attivo, possiamo fare una distinzione tra:

1. posizione estensiva del Provider, dove per qualificare il Provider come attivo è sufficiente l'indicizzazione dei contenuti multimediali immessi dagli utenti [57], oppure l'inserimento dei messaggi personalizzati;
2. posizione restrittiva del Provider, dove il prestatore del servizio non interviene in alcun modo sul contenuto caricato dall'utente, ma si limita solamente a sfruttarne la presenza commerciale sul proprio sito. In tal caso dovrà essere esclusa la natura di hosting provider attivo.

Arrivando poi al ruolo dell'*hosting provider passivo*, questo viene considerato come quella figura che non si interessa direttamente dei file e dei contenuti da esso veicolati, anzi ma si limita solamente a sfruttarne commercialmente la loro presenza sul proprio sito.
Si tratta di provider che forniscono principalmente uno spazio sui server senza un coinvolgimento attivo nella gestione dei contenuti illeciti.
Facciamo, pertanto, riferimento ad una figura che non si occupa né di offrire servizi di supporto tecnico avanzato o di monitoraggio, né di fornire interventi, di loro iniziativa, per risolvere problemi tecnici.
Il Provider passivo può essere considerato come responsabile per non aver provveduto tempestivamente alla rimozione dei contenuti illeciti, o per aver continuato a pubblicarli, se ricorrono le seguenti condizioni:

- Se ha conoscenza legale dell'illecito;
- Se l'illiceità del contenuto è da lui possibilmente constatabile;

[57] In funzione del numero di click, della parola chiave, del titolo e della categoria di appartenenza.

- Se ha la possibilità di attivarsi con lo scopo di rimuovere i contenuti illeciti.

Per comprendere al meglio l'argomento in questione, verranno riportati alcuni casi pratici nel paragrafo seguente.

2.2.3) Categorie di responsabilità del Provider.

Una tra le principali questioni che si sono andate a sviluppare intorno all'argomento del ruolo e della responsabilità del provider riguarda la possibilità di configurare in capo a quest'ultimo una responsabilità penale per i contenuti illeciti, pubblicati da terzi, nella loro piattaforma, anche in seguito all'enorme espansione del mondo dei social media.
Quando parliamo di categorie di responsabilità del Provider, possiamo distinguerle nel seguente modo:

- Responsabilità commissiva, che a sua volta può essere scomposta in monosoggettiva e concorsuale;
- Responsabilità omissiva.

Partendo dalla *responsabilità commissiva*, sia la Giurisprudenza che la Dottrina ritengono congiuntamente che il provider non possa rispondere sempre per aver agevolato l'utente a commettere il reato, anzi, molte volte è lo stesso provider che può essere considerato responsabile in proprio per aver commesso proprio lui il reato.
Per quanto riguarda la *responsabilità commissiva monosoggettiva*, si va ad intendere la situazione in cui il provider viene coinvolto per aver commesso autonomamente una fattispecie criminosa, ossia quando ad esempio abbia permesso all'utente di caricare un contenuto illecito o comunque lo abbia mantenuto sulla piattaforma senza rimuoverlo
Un esempio pratico di responsabilità commissiva autonoma affronta il tema di un gestore di un sito di annunci sul quale una escort ha pubblicato alcuni contenuti inadatti ad un pubblico minorenne per sponsorizzare la propria attività.
La domanda che qui sorge è la seguente: il gestore del sito può essere considerato responsabile per aver lasciato che la ragazza pubblicasse quei contenuti, ovvero perché non ha provveduto a rimuoverli?

Qui si tende ad escludere la responsabilità del gestore del sito di annunci, facendo ricorso alla distinzione tra favoreggiamento della prostituzione e favoreggiamento della prostituta.

In breve, quindi, il provider non può essere considerato responsabile se si limita a sfruttare economicamente i contenuti pubblicati dalla prostituta sul suo sito, ma lo diventa se invece va a coadiuvare tale attività, ad es. mettendo a disposizione servizi di videochat erotiche o di "*prostituzione a distanza* [58].

Passando ora alla *responsabilità per concorso attivo nel reato commesso dall'utente*, anche conosciuta come *responsabilità concorsuale*, la domanda qui che dobbiamo porci è la seguente: a che condizioni il provider può rispondere a titolo di partecipazione nel reato commesso dall'utente?

Per rispondere a questa domanda possiamo avanzare due soluzioni:

1. la prima, secondo la quale il contributo atipico del fornitore del servizio soggiace alle regole comuni sul concorso di persone nel reato. In parole povere è sufficiente che venga realizzato un illecito e che l'azione del provider si traduca in un'agevolazione, senza la quale il reato sarebbe stato comunque commesso, ma con maggiori difficoltà;
2. la seconda invece, si basa sul presupposto che, per rispondere a titolo concorsuale, il Provider deve partecipare alla condotta criminosa mediante un dolo di partecipazione molto intenso.

Con lo scopo di comprendere al meglio l'argomento in questione, si affronterà di seguito un caso di Giurisprudenza, considerato come il "leading case" italiano nel campo della responsabilità commissiva, ossia: "*Google v. Vividown* [59]".

Si tratta di un caso avvenuto in Italia nel 2013 e che ha visto scontrarsi il noto Provider di servizi di hosting, e-mail, motore di ricerca e video in streaming Google, e l'associazione benefica Vividown.

[58] Per prostituzione a distanza si intende l'esercizio dell'attività della prostituta mediante l'utilizzo di videocamere, impianti audiovisivi […] Secondo la Corte di Cassazione (sent. n. 37188 del 19/10/2010), lo spettacolo erotico in webcam è prostituzione nel momento in cui c'è una correlazione diretta tra la richiesta del cliente (ad esempio, quella di spogliarsi) e il comportamento posto in essere dalla ragazza in webcam.

[59] Cass. pen., Sez. III, 17 dicembre 2013 (dep. 3 febbraio 2014), n. 5107;

La vicenda ha inizio da una pubblicazione di un filmato, sulla piattaforma di Google Video, che ritrae un ragazzo disabile mentre era oggetto di bullismo da parte di alcuni compagni di classe, i quali, contestualmente, pronunciavano affermazioni ingiuriose nei confronti dell'associazione Vividown.
I vertici di Google Video vennero accusati di non aver impedito il delitto di diffamazione (art. 595 co.3 c.p.) nei confronti del minore e dell'associazione, di aver eseguito un illecito trattamento dei dati personali (art. 167 D.lgs. 196/2003).
Nella sentenza di primo grado, il Tribunale di Milano assolveva i vertici di Google dal concorso omissiva del delitto di diffamazione, in quanto non sussiste l'obbligo di prevenire i reati dei propri utenti, ma li ritenne responsabili per l'accusa di illecito trattamento di dati personali, visto che non avevano provveduto ad informare preventivamente i propri utenti riguardo agli obblighi nei confronti della trattazione dei dati personali.
La questione centrale riguarda quindi la responsabilità penale per ingiurie e bullismo sorta in capo ai vertici di Google Video.
Sebbene resti escluso un dovere di verifica da parte dell'ISP sul contenuto dei video e in particolare, l'onere di controllare che gli uploader abbiano ottenuto il consenso al trattamento dei dati personali dagli eventuali interessati, occorre chiedersi quindi se il Provider sia tenuto ad informare gli utenti sul necessario rispetto della normativa in materia di privacy e de rischi che si corrono in caso di mancata ottemperanza, e se detta omissione possa configurare un illecito trattamento dei dati.
Nella sentenza di primo grado, il Tribunale di Milano ha appunto affermato che non si stava parlando di mancata acquisizione del consenso, ma del mancato avviso degli uploader che il trattamento di dati altrui richiede il consenso.
La Corte di Appello ha confermato l'assoluzione per l'accusa di diffamazione, ma ha rigettato l'accusa in relazione all'illecito trattamento dei dati personali, assolvendo i manager anche sotto quel punto di vista, affermando che il provider che offre il servizio di upload va a beneficiare di limitazioni di responsabilità previste dagli artt. 16 e 17 del D.lgs. 70/20003 [60].
La procura generale ha quindi fatto ricorso in Cassazione, riportando le argomentazioni precedentemente citate. La Suprema Corte ha rigettato ogni questione di legittimità, ritenendo che Google, in base in base a quanto disposto dall'art. 167 D.lgs. 196/2003, non

[60] Vedi par. 2.2.1 "attività dell'isp" e par. 2.2.2 "hosting provider attivo e passivo, art.17 d.lgs. 70/2003".

abbia alcun obbligo o dovere di sorveglianza sui contenuti pubblicati dagli utenti, né tantomeno di informare gli uploader sui doveri loro incombenti in caso di pubblicazione di contenuti illeciti.
Nonostante vi sia stato un trattamento illecito di dati, tale illecito è ascrivibile solo agli uploader e non all'Host Provider (manager di Google Video), il quale non conosceva il contenuto illecito e che, non appena avvisato dalle autorità, ha provveduto tempestivamente alla sua rimozione.

Volgendo ora lo sguardo verso la r*esponsabilità omissiva*, notiamo come sia la Dottrina che la Giurisprudenza rifiutino l'idea che l'ISP sia titolare di una posizione di garanzia penalmente rilevante.
Al riguardo si è parlato proprio di escludere l'esistenza di un obbligo di impedimento, per evitare che il provider assumesse un ruolo basato sulla censura della rete.

a) Ciò che la Dottrina ha ritenuto riguardo la posizione del provider è la mancanza, prima di tutto, di una norma che fondi un generale obbligo di vigilanza degli utenti della rete, visto che l'art. 17 D.lgs. 70/2003 sancisce il principio opposto;
b) Se ci fosse questo obbligo generale di vigilanza non sarebbe esigibile, vista l'enorme quantità di dati che transitano ogni secondo sul web;
c) Manca un potere impeditivo specifico, sia dal punto di vista giuridico che da quello fattuale.

Dalla lettura congiunta degli artt. 14,15 e 16 del D.lgs. 70/2003, si ricava che tutti i provider sono tenuti ad impedire l'accesso ai dati o a rimuoverli, solo a seguito della richiesta da parte della pubblica autorità o in presenza di materiale palesemente illecito.
Negli altri casi la rimozione di materiale potrebbe dar luogo ad un obbligo risarcitorio nei confronti dell'utente ingiustamente censurato dal punto di vista fattuale, sarebbe eccessivo fondare la posizione di garanzia sull'assunto dell'esercizio di un'attività ex-se pericolosa. L'astratta possibilità che si commettano reati online non può rendere pericolosa solo la necessaria e fondamentale attività di connessione di servizi per tutti i potenziali utenti della rete.
Con riferimento alla mancanza di un potere impeditivo, possono essere avanzate due considerazioni:

- Da un lato la gestione da parte del Provider può non integrare gli estremi di un'attività pericolosa basata sull'imposizione di un obbligo di attivazione, dal momento che la mera fornitura di un accesso a internet rappresenta una condotta eccessivamente distante rispetto alla soglia del pericolo di realizzazione del fatto tipico, che non può ritenersi naturale sviluppo dell'agire precedente del provider, consistendo invece esclusivamente nell'autonoma azione, volontaria e consapevole di un terzo.
- Dall'altro lato invece, la gestione di un sito nel quale chiunque ha la possibilità di caricare un proprio contenuto con una semplice operazione di upload, può essere considerato come esercizio di attività pericolosa per i beni altrui.

In tutto ciò la Giurisprudenza è ferma nel ritenere che il provider non rivesta una posizione di controllo penalmente rilevante, come nel caso "Google v Vividown".
Quindi sia la Giurisprudenza che la Dottrina maggioritaria sostengono che il provider, nella maggior parte dei casi, non possa rispondere penalmente per omissione, ma non in tutti.
Si passerà ora ad un'analisi della *responsabilità omissiva propria.*
Quando parliamo di responsabilità omissiva propria facciamo riferimento alla fattispecie in cui il Provider risponde personalmente per non essersi attivato.
Quando al Provider viene imposto un obbligo di segnalazione da parte delle autorità, e questi non si attiva, può rispondere anche della violazione di altre norme, come ad es. il favoreggiamento personale (art 378 c.p.).
Immaginiamo infatti che un Provider conosca l'utente che ha pubblicato e diffuso in rete il contenuto diffamatorio e di conseguenza riceva un ordine, da parte delle autorità competenti, di fornire l'indirizzo IP del reo.
Se esso non adempie all'ordine e decide di non fornire l'indirizzo IP richiesto, allora può rispondere di favoreggiamento in forma omissiva.
Può verificarsi anche il caso in cui al Provider venga richiesto espressamente, dalle autorità competenti, di rimuovere il materiale illecito presente nella sua pagina web. In caso di inadempimento alla richiesta da parte del Provider, questi potrà essere esposto a gravi conseguenze, quali:

- Provvedimenti giurisdizionali, come ad esempio un'ordinanza del giudice civile. La loro violazione può integrare il "delitto di mancata esecuzione dolosa di un provvedimento del giudice" (art. 388 c.p.) soltanto se il fornitore del servizio compia atti fraudolenti diretti ad eludere i predetti obblighi. Diversamente, il fatto sarà inquadrato nella "contravvenzione" di cui all'art. 650 c.p. che punisce (anche a titolo di colpa), l'inosservanza di provvedimenti dell'autorità emessi, come nel caso di specie, per ragioni di giustizia.
- Provvedimenti dell'autorità amministrativa o di pubblica sicurezza, in questo caso sarà sanzionato unicamente ai sensi dell'art. 650 c.p., a condizione che il provvedimento amministrativo sia ricondotto a una delle categorie previste dalla norma.

2.3) Alcuni casi pratici di Giurisprudenza.

Premessa

In questo paragrafo conclusivo del capitolo 2 si andranno a trattare alcuni casi di Giurisprudenza avvenuti in epoca abbastanza recente, con lo scopo di comprendere l'argomento della responsabilità del Provider non solo da un punto di vista teorico ma anche in una sua applicazione pratica.

I casi riportati in questo paragrafo sono due, ossia:

1. "*RTI (reti televisive italiane) v. Yahoo!italia"*, n. 7709/2019 Corte di Cassazione, il quale verrà suddiviso in 3 parti principali, andando in ordine cronologico, partendo dagli avvenimenti del 2011, passando per quelli del 2014 e arrivando infine alla sentenza finale del 2019;
2. "Sabam v. Netlog" n.360/2010 CGUE.

Analizzando rispettivamente i casi presi in esame, verrà mostrato l'iter decisionale che ha portato le Corti a prendere determinate decisioni.

2.3.1) RTI v. Yahoo!Italia. n. 7709/2019

Si tratta di uno dei principali casi di Giurisprudenza Italiana che hanno coinvolto la figura del Provider e le sue responsabilità. Il caso in questione, come accennato nella premessa, si suddivide in 3 diversi gradi processuali, avvenuti rispettivamente nel 2011, 2014 e 2019, e coinvolge le seguenti parti:

- il gruppo RTI, ossia Reti Televisive Italiane, gruppo televisivo appartenente a Mediaset;
- la compagnia Yahoo!Italia s.r.l., il famoso portale web nato nel 1994 e appartenente al mondo del business & consumer.

Il caso in esame risale alla Sentenza di primo grado del 2011 da parte del Tribunale di Milano, il quale riconobbe Yahoo quale provider attivo e in quanto tale responsabile per aver diffuso illecitamente e senza autorizzazione contenuti coperti da copyright.
Il caso poi continuerà in appello nel 2014 e si concluderà in Cassazione nel 2019.

1. *RTI v. Yahoo!Italia, 2011.*

Il caso in questione ha inizio con la Sent. n. 10893/2011 con la quale il Tribunale di Milano ha condannato la compagnia Yahoo per aver commesso la violazione di alcuni diritti d'autore appartenenti a Reti Televisive Italiane.
Secondo il Tribunale di Milano la violazione citata si fondava su una serie di contenuti e spezzoni appartenenti a trasmissioni televisive quali ad es. "Striscia la Notizia", "Il Grande Fratello", "Amici" […] i quali erano stati caricati dagli utenti sul portale web di Yahoo!Italia.
Di conseguenza la compagnia Yahoo!Italia, attraverso i suoi legali, ha avanzato una difesa incentrata sulla limitazione della responsabilità prevista dall'art.16 co.1 D.lgs. 70/2003, secondo la quale:
"Nella prestazione di un servizio dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanza che rendono manifesta l'illiceità dell'attività o dell'informazione;
b) Non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

Il Tribunale di Milano, dopo aver osservato attentamente le difese avanzate dai legali dell'imputato, è arrivato alla conclusione che: "*deve essere ritenuta inapplicabile la limitazione di responsabilità prevista dall'art.16 D.lgs. 70/2003* [61]*, poiché non è possibile ritenere Yahoo!Italia s.r.l. come un soggetto passivo e neutro rispetto all'organizzazione alla gestione di contenuti immessi dagli utenti, anzi, si deve ritenere che il provider offra quantomeno un servizio di Hosting e tragga dall'organizzazione dei contenuti un sostegno finanziario in ragione allo sfruttamento pubblicitario connesso alla presentazione di tali contenuti* [62] ".

La Corte sosteneva, dunque, che la compagnia Yahoo!Italia non potesse essere ritenuta come un mero prestatore di servizi tecnici, automatici e passivi, per i seguenti motivi:

- Prima di tutto, il soggetto in questione trae un profitto dalla presenza di questi contenuti caricati dagli utenti, attraverso la vendita dei servizi pubblicitari collegati a tali contenuti.
- Le condizioni generali del servizio prestato prevedono inoltre che la compagnia Yahoo!Italia s.r.l. acquisisca, in virtù del caricamento sul sito il diritto di riprodurre e distribuire i contenuti attraverso qualsiasi mezzo di comunicazione e di intervenire su di essi manipolandoli per finalità pubblicitarie;
- Le condizioni generali prevedono inoltre una garanzia in favore di Yahoo per qualsiasi danno arrecato a terzi, derivante dalla pubblicazione di contenuti caricati dall'utente;
- Yahoo, inoltre, ha messo a disposizione per gli utenti un servizio che permette la visione di video correlati.

La motivazione avanzata dal Tribunale si basa sulla pronuncia n. 7680/2011, emanata precedentemente dalla medesima Corte. In questa pronuncia il Tribunale assolveva la società RTI e condannava la compagnia "IOL" (*Italia Online*[63]), la quale possedeva una piattaforma telematica che consentiva la condivisione dei contenuti audio/video inviati dagli utenti.

[61] Vedi pagina precedente

[62] Cass. Civ. Sent. n. 10893/2011;

[63] Italia online è una società italiana, fondata nel febbraio 2013, che opera nel campo del marketing digitale e della comunicazione online. Ha ottenuto il record come prima azienda digitale italiana per numero di utenti unici in media al giorno.

RTI ha contestato l'illecita presenza su detta piattaforma di filmati di proprietà di essa attrice, in particolare, nella sezione video del Portale IOL, era possibile eseguire anche una ricerca di frammenti video del materiale di pertinenza dell'attrice, inserendo semplicemente il tiolo di una di queste trasmissioni nella sezione
"*key-words* [64]". Questo fatto, secondo l'attrice, ha conseguentemente comportato diverse violazioni della normativa in tema di diritto d'autore.
Come accennato in precedenza in RTI v. Yahoo!Italia, anche in questo caso la difesa ha invocato l'applicabilità della limitazione della responsabilità del Provider, prevista dall'art. 16 D.lgs. 70/2003, ma anche qui ne è stata rilevata l'applicabilità da parte del Tribunale di Milano. Quindi, sia nel caso "RTI v. Yahoo!Italia", sia nel precedente "RTI v. IOL", la Corte ha stabilito che: "*Premessa l'impossibilità anche per il prestatore di servizi di "hosting attivo" di poter procedere ad una verifica preventiva del materiale immesso quotidianamente dagli utenti (non potendosi ritenere tale verifica quale comportamento effettivamente esigibile per la complessità tecnica che un tale controllo richiederebbe, anche in relazione al possibile conflitto con forme di libera manifestazione del pensiero o di utilizzazione di contenuti protetti dal diritto d'autore per i quali ricorrano ipotesi di utilizzazione libera), deve essere attribuito opportuno rilievo alla ricezione di un atto di diffida, dato che l'informazione sulla presenza di diritti di terzi determina l'insorgenza, in capo al prestatore dei servizi, dell'obbligo di attivarsi ancora prima della ricezione da parte dell'autorità giudiziaria o amministrativa dell'ordine di rimozione del contenuto illecito* [65]".
Nel caso di Yahoo, pertanto, la compagnia aveva già ricevuto una diffida da parte di RTI, con la quale si andavano a segnalare i contenuti illeciti presenti che violavano i diritti d'autore e, si richiedeva la loro conseguente rimozione.
Una volta attestata la violazione dei diritti d'autore, sopra menzionati, da parte di Yahoo!Italia, è stato imposto alla compagnia quanto segue:

- il divieto di trasmettere nuovamente tali contenuti;
- il pagamento di euro duecentocinquanta per ogni video non rimosso e per ogni giorno di ritardo nell'esecuzione del provvedimento in questione.

[64] Per "key words" si intende l'inserimento di quelle parole chiave che danno la possibilità al programma in questione di ricercare con maggiore semplicità l'argomento richiesto.
[65] Cass. Civ. Sent. 10893/2011/; Riv. Dir. ind. 2011, 6, II, 364 nota

2. RTI v. Yahoo!Italia, 2014

Come detto in precedenza, il caso in questione ha trovato infine soluzione nel 2014, con la Sent. n. 11295. Tale pronuncia del 2014 fece molto eco, poiché lo stesso Tribunale che aveva precedentemente condannato la compagnia Yahoo!Italia nel 2011, si pronunciò, questa volta in senso opposto e assolvendo la Compagnia dalle accuse che gli erano state mosse. Secondo il Tribunale di Milano, tornando alla pronuncia del 2011, l'attrice RTI ha impostato l'intera vicenda a suo favore. L'argomentazione che è stata riportata nella pronuncia del 2014 va a ribaltare completamente la considerazione della figura del Provider, il quale nel 2011 veniva ritenuto come "non neutro/attivo", secondo la lettura dell'art.16 D.lgs. 70/2003 e, quindi, responsabile per le attività illecite compiute sulla sua piattaforma. La nuova lettura ha interpretato la definizione di "motore di ricerca [66]" quale attività di caching e non di hosting; il caching, disciplinato dall'art. 15 D.lgs. 70/2003, fa riferimento alla temporanea memorizzazione di dati e informazioni, contrassegnandosi quindi per la neutralità e passività rispetto alle informazioni trattate. Questa nuova considerazione, fornita nel nuovo giudizio, si basa su un ragionamento prodotto dalla Corte facendo ricorso alla responsabilità prevista dall'art. 17 d.lgs. 70/2003, secondo il quale: "il provider non è assoggettato ad un obbligo generali di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite". Quindi, secondo il disposto dell'art.17 D.lgs. 70/2003, la compagnia Yahoo!Italia non ha effettivamente violato la condizione di neutralità prevista e, conseguentemente, non è tenuta ad alcun obbligo di sorveglianza sulle informazioni che trasmette o memorizza. Secondo le difese avanzate dalla difesa dell'imputato, la Compagnia Yahoo!Italia, nello svolgimento delle sue funzioni, ha sempre offerto sulla sua piattaforma un servizio video conosciuto con il nome di: "*Yahoo! Search*[67]".

[66] L. Manna: "Responsabilità dell'ISP: Yahoo vince il secondo round contro RTI", MartiniManna & Partners, 2014.

[67] Yahoo!search è un servizio, offerto dalla piattaforma di Yahoo, che nasce come un'evoluzione del precedente Yahoo!video. A primo impatto i due possono sembrare la stessa cosa, ma sono molti gli aspetti che li differenziano, ad es:

- la funzione Yahoo!video implica dei servizi di organizzazione, pubblicazione e manipolazione diretta dei contenuti da parte del Provider, il quale va ad assumere quindi un ruolo di hosting attivo;

Questo servizio non è basato sull'elaborazione dei dati, bensì sull'ottimizzazione del servizio di ricerca, attraverso funzioni di "*ebbeding del video*[68]" e di "auto-completamento[69]".

Tale funzione concessa dalla piattaforma, non va in sé e per sé ad alterare le condizioni di neutralità del prestatore del servizio rispetto alle informazioni fornite.

Tale Sentenza fu argomento di molte discussioni, sia in Dottrina che in Giurisprudenza, a causa del verdetto che ha portato al capovolgimento della pronuncia del 2011.

Si arriverà infatti dinanzi alla Suprema Corte di Cassazione nel 2019.

3. RTI v. Yahoo!Italia, 2019

Il caso di cui al presente paragrafo si conclude con la pronuncia emanata dalla Corte di Cassazione nel 2019.

La questione qui vede la società RTI ricorrere in Cassazione avverso la pronuncia emanata nel 2014 da parte del Tribunale di Milano, il quale, come precedentemente trattato, aveva già rigettato la domanda proposta da RTI, accertando invece che l'attività svolta dalla compagnia di Yahoo!Italia, tramite la funzione Yahoo!search, appartenesse al ramo del caching e non a quello dell'hosting.

Il ricorso avanzato da RTI poneva le proprie basi sui seguenti cinque motivi di diritto:

a) erronea valutazione, da parte del Tribunale di Milano, del ruolo di Yahoo!search e della normativa che va a disciplinare l'attività del catcher;
b) Anche se il prestatore del servizio avesse fornito una mera attività di caching, una volta a conoscenza dei contenuti illeciti, non ha comunque provveduto alla loro tempestiva rimozione. Quindi in questo caso "non facciamo più riferimento ad un generale ed insussistente obbligo di vigilanza preventiva, ma della violazione

---

- i servizi svolti mediante la funzione Yahoo!search vengono invece fatti rientrare nell'attività di caching, disciplinata dall'art. 15 D.lgs. 70/2003, in quanto la funzione di motore di ricerca implica l'organizzazione in un elenco di siti pertinenti ai criteri di ricerca indicati dall'utente interrogante, attraverso la fornitura di link che consentono la connessione con ciascuno di essi. Tramite questa funzione viene quindi eseguita una copia temporanea delle copie dei siti all'interno di una cache, ossia un'area di memoria estremamente veloce ma con scarsa grandezza e capacità di immagazzinamento.

[68] Con il termine "ebbeding" si intende l'incorporazione di un oggetto in un altro o, più facilmente, di un contenuto digitale su di una diversa piattaforma, e così via.

[69] "L'autocompletamento" è una funzione in possesso a molti sistemi informatici, che da la possibilità di intuire automaticamente la parola o l'espressione che si vuole digitare tramite la tastiera, già dalle prime lettere.

dell'obbligo di ponderare la richiesta ricevuta dal terzo titolare del diritto, assumendone le conseguenze, quale imprenditore ex art. 2082 c.c., in termini di responsabilità, ove la richiesta sia fondata ed egli non si sia attivato per rimuovere i contenuti illeciti, dovendo essere in grado di valutarne i limiti".

c) La sentenza impugnata ha sbagliato a ritenere che la diffida stragiudiziale non sarebbe stata idonea a fondare l'obbligo di controparte di rimuovere i contenuti illeciti, in quanto non sufficientemente specifica nell'indicare i singoli filmati;
d) Nella sentenza impugnata non era presente alcuna pronuncia riguardo l'altrui dovere di attivarsi, cosa che invece era già stata menzionata nella Sent. n. 10893/2011;
e) Nella sentenza impugnata non c'è alcuna menzione neanche della domanda che ha lo scopo di ordinare alla controparte la disabilitazione o de-indicizzazione all'accesso a tutti i siti internet estranei ad essa attrice.

Secondo quanto sostenuto dalla ricorrente, Yahoo!search ha effettuato un intervento di tipo selettivo e per nulla necessario alla normale operatività del motore di ricerca sui contenuti (funzioni di "ebbeding" e di "auto-completamento").
Quindi in breve, secondo RTI, il Provider in questione avrebbe perso la sua posizione di neutralità rispetto alle informazioni memorizzate, esercitando appunto un controllo effettivo su di esse.

La Suprema Corte di Cassazione è arrivata all'esito finale con la Sent. n. 7709/2019, basandosi sul rigetto del ricorso proposto da RTI e sulla conferma di ciò che era stato precedentemente stabilito dalla Tribunale di Milano.
Il primo motivo di ricorso viene considerato come infondato poiché la Corte ha ritenuto che:"*Il ruolo del prestatore dei servizi non ha varcato i limiti della prestazione di mero catching, questo perché la funzione "yahoo!search" si limita solo a svolgere il ruolo di mero motore di ricerca, consistente nel cercare e organizzare un elenco di siti pertinenti ai criteri di ricerca indicati dall'utente interrogante, fornendo i link che consentono la connessione con ciascuno di essi* [70]".

[70] Sent Cass. Civ. n. 7709/2019

Per quanto riguarda i restanti motivi, la motivazione avanzata dalla Corte ribadisce ciò che è stabilito dall'art. 15 D.lgs.70/2003, analizzando come la figura del cacher e la sua responsabilità siano molto diversi e distaccati da quelli dell'hosting provider.
Quindi il Tribunale ha statuito che il prestatore non risponde dell'illecito poiché non ha oltrepassato i limiti della responsabilità, bensì ha assolto ai doveri di cui all'art. 17 co. 2, con riferimento alla trasmissione della diffida del titolare del diritto d'autore alla Procura competente.
Il quarto motivo, infine, è stato ritenuto inammissibile e il quinto come infondato.
La Corte ha rigettato per intero il ricorso di RTI, confermando la pronuncia del Giudice di primo grado.
È importante quindi notare come, nel caso in esame, venga ricalcata la differenza tra il Provider che svolge una funzione di caching e quello che invece presta servizi di hosting, differenza che spesso può risultare molto sottile.
La compagnia Yahoo!Italia, mediante l'apposita funzione Yahoo!search, non è intervenuta direttamente sui contenuti che venivano da essa veicolati attraverso la piattaforma, bensì si è limitata a svolgere solamente il ruolo di semplice motore di ricerca.
Come stabilito dall'art. 16 D.lgs. 70/2003, si parla di "hosting provider attivo" quando il prestatore offre un servizio di memorizzazione stabile e va direttamente ad interagire sui contenuti da esso veicolati, offrendo funzioni di indicizzazione, archiviazione stabile e pubblicizzazione.
La compagnia in questione non ha svolto nessuna di queste funzioni, in quanto si è limitata solamente ad organizzare, come detto, questi contenuti in un elenco di siti, fornendo link che consentono la connessione con ciascuno di essi.
L'attività svolta da Yahoo!Italia rispecchia quindi perfettamente quella di un cacher, il quale, come stabilito dall'art. 15 D.lgs. 70/2003, non offre servizi di indicizzazione o di memorizzazione stabile.
In conclusione, quindi, secondo la ricostruzione fornita dalla Cassazione, Yahoo!Italia non può essere considerato come un "hosting provider attivo" poiché la funzione da esso svolta si traduce in realtà in una mera attività di caching che, lo esonera dalle responsabilità previste per l'hosting provider e gli garantisce così una posizione di neutralità rispetto ai contenuti che vengono da esso veicolati.

2.3.2) Sabam v. Netlog C-360/10 CGUE, Sez. III

Il caso in esame si sviluppa a livello Internazionale e tratta la tematica della responsabilità del Provider legata all'utilizzo di opere dell'ingegno protette dal diritto d'autore.

È innanzitutto opportuno descrivere bene i fatti a base della vicenda, per comprendere appieno lo sviluppo e gli esiti.

Le parti interessate nel seguente caso sono due, ossia:

- La "Société d'Auteurs Belge – Belgische Auteurs Maatschappij", conosciuta con l'acronimo di Sabam, una società Belga che gestisce e rappresenta gli autori, i compositori e gli editori di opere musicali. Rivestendo tale ruolo, la Sabam è quindi investita della responsabilità e del compito di autorizzare l'utilizzo, da parte di soggetti terzi, delle opere dell'ingegno presenti nel suo repertorio.
- Netlog, un social network creato nel 2006, che gestiva una piattaforma digitale dove gli utenti, all'epoca principalmente giovani, potevano caricare foto, video, informazioni sulla propria vita […] attraverso il loro profilo personale [71]. Offriva anche la possibilità agli utenti di creare dei gruppi, chiamati: "clan", all'interno dei quali potessero interagire tra di loro condividendo video, messaggi e contenuti.

La Sabam, nel 2009, ha mosso un'accusa nei confronti di Netlog, sostenendo che il social network in questione ha fornito, agli utenti iscritti, la possibilità di caricare sul proprio profilo contenuti audiovisivi e musicali protetti da diritto d'autore, i quali appartenevano al repertorio della società Belga.

La Sabam ha cercato di proporre inizialmente un metodo di risoluzione pacifico, proponendo a Netlog la stipula di una convenzione che garantiva al social network la possibilità di continuare ad utilizzare il materiale protetto dal diritto d'autore attraverso il pagamento di un compenso alla società Belga.

[71] Il profilo personale di un utente, iscritto ad un social network, rappresenta il luogo digitale nel quale il soggetto va a riportare le proprie informazioni personali. Il profilo viene visto quindi come un insieme di dati relativi ad un utente di un sistema informatico. Per poter creare il profilo personale si deve prima di tutto creare un account mediante il quale l'utente andrà ad iscriversi presso il social network e verrà identificato in base alla fornitura di un "nome utente" (ossia il nome con il quale verrà riconosciuto l'utente sul social) e una password, che gli permetterà di mantenere in sicurezza le proprie informazioni da soggetti terzi o fughe di dati.

Netlog ha però rifiutato la proposta e conseguentemente la Sabam ha avanzato un atto di citazione dinanzi al Tribunale di Primo Grado Belga.

Le richieste avanzate dalla società Belga erano le seguenti:

- La cessazione immediata del comportamento illecito posto in essere da Netlog;
- il pagamento di euro mille per ogni giorno di ritardo nell'adempimento del primo obbligo.

La Compagnia Netlog ha conseguentemente presentato opposizione a tale citazione, costituendosi in giudizio e sostenendo che l'eventuale accettazione delle richieste avanzate dalla Sabam avrebbe rappresentato un'imposizione di un obbligo generale di sorveglianza alla piattaforma.
Secondo la società Belga tale obbligo, in base a quanto sostenuto dall'art. 21 p. 1 L. 11/2003, norma che recepisce l'art. 15 Dir. 31/2000, non può sussistere.
Il caso verrà poi rimesso dal Tribunale Belga alla Corte di Giustizia dell'Unione Europea per questioni di interpretazione normativa.
La questione al centro del dibattito riguardava la possibilità che le norme UE contrastassero l'ingiunzione rivolta da un giudice nazionale ad un prestatore di servizi di hosting (quale gestore di una rete sociale).

I motivi che hanno poi spinto la Corte a prendere le sue decisioni sono i seguenti:

1. coloro che sono titolari di diritti di proprietà intellettuale, hanno la possibilità di chiedere al gestore di una rete sociale l'emanazione di un provvedimento inibitorio nei confronti degli utenti che violano i diritti in questione nell'utilizzo dei servizi offerti;
2. la Netlog ha la possibilità di memorizzare, direttamente sui propri server, le informazioni fornitegli dagli utenti;
3. la predisposizione del sistema di filtraggio in questione prevede che il prestatore di servizi di hosting (in questo caso Netlog) debba occuparsi dell'identificazione, tra i file memorizzati sui suoi server, di tutti i documenti che possono contenere opere o creazioni protette da diritti di proprietà intellettuale. L'hosting provider in questione ha poi il compito di determinare quali, tra i suddetti file, siano messi a

disposizione del pubblico in maniera illecita, con il fine ultimo di bloccare la loro diffusione.

Una sorveglianza di tale portata richiederebbe pertanto un'osservanza generalizzata e continua dei file memorizzati dagli utenti presso il gestore della rete sociale.
Come stabilito dall'art. 15 della Direttiva E-commerce:
"*Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite* [72]".
Inoltre, se si ponesse in atto una sorveglianza del genere, questo implicherebbe un controllo, non solo sulle violazioni già commesse in passato, ma anche su quelle future.
Un'ingiunzione di tale tipo andrebbe quindi a causare una grave violazione della libertà d'impresa della compagnia Netlog e conseguente lesione dei diritti fondamentali dei suoi utenti.
Quindi in conclusione la CGUE ha dichiarato che le Direttive n.2000/31(e-commerce), n.2001/29 [73] e n.2004/48 [74], lette in combinato disposto, devono essere interpretate nel senso che ostacolano all'ingiunzione, rivolta da un giudice ad un prestatore di servizi di hosting, di predisporre un sistema di filtraggio delle informazioni, sistema che venga applicato indistintamente a tutti gli utenti, a titolo preventivo, senza limiti di tempo e a spese esclusive del prestatore.
Se venisse applicato un sistema di filtraggio come quello sopra menzionato si rischierebbe anche di ledere la libertà di informazione generale, in quanto tale sistema potrebbe non essere in grado di distinguere adeguatamente un contenuto lecito da uno illecito; questo causerebbe quindi il rischio di bloccare contenuti perfettamente leciti.

[72] Art. 15 co.1 Dir. n. 31/2000
[73] Direttiva n. 29 del 2001, ossia la direttiva sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nelle società dell'informazione
[74] Dir. n. 48 del 2004, ossia la direttiva sul rispetto dei diritti di proprietà intellettuale, facendo riferimento espressamente anche agli strumenti giuridici a disposizione dei titolari dei diritti.

PARTE III

3) recenti interventi normativi

Con il seguente capitolo si intende ripercorrere e analizzare come il recente quadro normativo Europeo e Nazionale sia intervenuto sin qui sulla regolamentazione del ruolo e della responsabilità del Provider.

Nel capitolo in questione sono riportati alcuni regolamenti e strategie economico-politiche che sono state promosse ed approvate negli ultimi anni all'interno dell'Unione Europea e che hanno lo scopo di illustrare come il ruolo e le attività del provider devono essere adattati al nuovo quadro economico-giuridico europeo e ai cambiamenti richiesti ed applicati dalle recenti politiche UE.

Il capitolo in questione ha quindi lo scopo di fornire un'analisi dettagliata dello scenario giuridico e normativo sviluppatosi finora intorno all'argomento in esame, verificando il modo in cui i providers hanno dovuto adattare il loro ruolo e le loro attività per garantire un'uniformità generale delle politiche europee.

Gli ambiti che verranno trattati sono i seguenti:

1. Il Regolamento sulla Net Neutrality, n.2120 del 2015, adottato dal Parlamento Europeo con lo scopo da un lato, di stabilire quali siano le misure adatte a garantire l'accesso ad una rete internet aperta, dall'altro invece di modificare la precedente Direttiva 2002/22/CE relativa al servizio universale e degli utenti in materia di reti e di servizi di comunicazione elettronica. Tale ultima modifica riguarderà, come vedremo successivamente, anche il Regolamento UE n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'UE;
2. La DSM Strategy, ossia la strategia per il mercato unico digitale, adottata dall'Unione Europea a partire dal 2015, con il fine di perseguire alcuni obiettivi, come ad es: promuovere la diffusione dell'e-commerce nell'UE, aumentare le capacità difensive dell'Unione nell'ambito degli attacchi informatici ed aiutare i cittadini e le piccole-medio imprese a sfruttare al meglio la digitalizzazione e le nuove tecnologie, il tutto ricalcando l'importanza del ruolo che il provider ricopre a riguardo. La DSM Strategy si distingue in molti aspetti dal Regolamento sulla "Net Neutrality" precedentemente menzionato, ma ciò che li lega è la promozione

di un ambiente digitale libero e senza barriere all'interno dell'UE, con riferimento al commercio elettronico, i servizi di connessione e la digitalizzazione.

Essa comprende anche il Digital Service Act (DSA) e il Digital Market Act (DMA), due normative recentissime frutto di ingenti sforzi e di accurate negoziazioni in ottica della realizzazione di un mercato unico europeo dei servizi.

3. La recente Delibera n. 9/2023 Agcom, con riferimento alla possibilità di intervento dell'Autorità per le Garanzie nelle Comunicazioni sulle attività del Provider, analizzando a riguardo tutti i possibili rischi e vantaggi che vi possono scaturire;
4. Il Dibattito sul c.d. "fair share", un criterio politico-economico basato sull'imposizione di una tassa/contributo nei confronti dei grandi operatori del web che da soli utilizzano circa il 50% del traffico internet.

   Tramite il "fair share" si intende quindi adottare il principio c.d. "senders pay", applicandolo al mondo delle Big Tech Europee, mettendo alla luce le conseguenze che possono derivare dall'adozione di una tale strategia. Il dibattito in questione è introdotto nel capitolo in esame con lo scopo di analizzare come in realtà l'adozione di un principio quale "senders pay", potrebbe tramutarsi in una limitazione del commercio elettronico e dei servizi di connessione, allontanandosi dall'obiettivo principale che l'Unione Europea intende raggiungere attraverso l'adozione di tale strategia, ossia il rafforzamento degli investimenti e il miglioramento del traffico in internet.

3.1) Regolamento (UE) n. 2015/2120, "Net Neutrality".

Il Regolamento (UE) n. 2015/2120 del Parlamento Europeo e del Consiglio del 25 novembre 2015, è una normativa che stabilisce misure riguardanti l'accesso ad una rete internet più aperta e ha lo scopo di promuove il principio della neutralità della rete, in base al quale l'accesso ad internet deve essere trattato in modo non discriminatorio, indipendentemente dal contenuto, dall'applicazione, dal servizio e dal mittente/destinatario

Tale normativa si basa sulla modifica della Direttiva 2002/22/CE, relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, e del Regolamento (UE) n. 2012/531 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione.

Partendo dall'accesso ad una rete internet aperta, le modalità attraverso le quali si intende raggiungere l'obiettivo in questione, sono le seguenti:

a) definire delle norme che abbiano lo scopo di garantire un trattamento equo e non discriminatorio della fornitura dei servizi di accesso a internet, andando allo stesso tempo a tutelare quelli che sono gli utenti finali e i loro diritti e ad eliminare le barriere poste al traffico in rete. I diritti in questione sono ad es. il diritto all'accesso ad informazioni e contenuti, con la possibilità di diffonderli indipendentemente dal tenore o dalla destinazione del contenuto [75].
b) Sostenere il principio della neutralità tecnologica, ossia non imporre né favorire l'utilizzo di un determinato tipo di tecnologia;
c) Far rispettare ai fornitori di servizi di accesso ad internet gli obblighi relativi a tale fornitura, vietandogli o almeno impedendogli di limitare la connettività ad alcun punto finale accessibile di internet;
d) Garantire agli utenti finali la possibilità di concordare con i fornitori di servizi di accesso ad internet, le tariffe adeguate ai dati trattati e alla velocità del servizio;
e) Imporre ai fornitori dei servizi di accesso a internet l'adozione di una disciplina di gestione del traffico non limitativa e/o discriminatoria. Le misure che andranno a violare queste limitazioni saranno vietate e sanzionate, a meno che non si rivelassero necessarie per la protezione dell'integrità e della sicurezza della rete stessa;
f) Garantire ai fornitori di contenuti la possibilità di poter offrire servizi diversi da quelli di accesso a internet, ma solo se le capacità della rete sono sufficienti a supportare questa fornitura aggiuntiva;
g) Indicare alle autorità nazionali quali sono gli obblighi in materia di monitoraggio e comunicazione che dovranno essere rispettati per garantire che gli utenti finali siano effettivamente in grado di esercitare i propri diritti;
h) Cercare di eliminare quelle che sono le differenze di costi tra le tariffe di roaming e le tariffe nazionali. Vengono applicate inoltre alcune regolamentazioni per i

[75] Art 3 co.1 Reg. 2120/2015: "*Gli utenti finali hanno il diritto di accedere a informazioni e contenuti e di diffonderli, nonché di utilizzare e fornire applicazioni e servizi, e utilizzare apparecchiature terminali di loro scelta, indipendentemente dalla sede dell'utente finale o del fornitore o dalla localizzazione, dall'origine o dalla destinazione delle informazioni, dei contenuti, delle applicazioni o del servizio, tramite il servizio di accesso a Internet*".

fornitori dei servizi di roaming, i quali, nell'esercizio delle loro attività, devono essere in grado di applicare a tali servizi una "politica di utilizzo corretto[76]".

Con riferimento, poi, al Regolamento (UE) n. 531/2012, l'obbiettivo posto alla base di questa normativa è quello di: "*ridurre la differenza tra i prezzi nazionali e quelli di roaming*[77]".

Secondo quanto enunciato nel Regolamento: "*non si può sostenere l'esistenza di un mercato interno delle telecomunicazioni se sussistono notevoli differenze tra i prezzi nazionali e i prezzi di roaming. Pertanto l'obbiettivo ultimo dovrebbe essere l'eliminazione della distinzione tra le tariffe nazionali e le tariffe di roaming e la conseguente istituzione di un mercato interno per i servizi di comunicazioni mobili*[78]"

Si tratta quindi di una normativa che per anni ha sostenuto la politica del c.d. "Roaming like at home", portata avanti poi dal Regolamento (UE) n. 2015/2120 sulla "Net Neutrality" con alcune modifiche, le seguenti[79]:

- Soppressione, nell'art. 2 par. 2, delle lettere i), l) e n) e aggiunta delle seguenti lettere:
    - r) "*prezzo al dettaglio nazionale*", una tariffa al dettaglio nazionale per unità del fornitore di roaming applicabile alle chiamate effettuate e ai messaggi SMS inviati (da e verso diverse reti pubbliche di comunicazioni all'interno dello stesso Stato membro) e ai dati consumati da un cliente; nel caso in cui non vi sia una specifica tariffa unitaria al dettaglio nazionale, si ritiene che il prezzo al dettaglio nazionale sia lo stesso meccanismo di tariffazione applicato al cliente per le chiamate effettuate e i messaggi SMS inviati (da e verso diverse reti pubbliche di comunicazioni all'interno dello stesso Stato membro), e i dati consumati nello Stato membro di tale cliente;

[76] La politica di utilizzo corretto dei servizi di roaming è un criterio/principio che nasce con lo scopo di prevenire qualsiasi utilizzo abusivo o anomale dei servizi di roaming al dettaglio, garantendo così una maggiore sicurezza e una più elevata trasparenza del servizio fornito.

[77] Reg. (UE) n. 531/2012 del Parlamento Europeo e del Consiglio del 13 giugno 2012, relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione, punto 2;

[78] Reg. (UE) n. 531/2012 del Parlamento Europeo e del Consiglio del 13 giugno 2012, relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione, punto 3;

[79] Art. 7 Regolamento 2120/2015: "modifiche del Regolamento UE n. 531/2012";

- s) "*vendita separata di servizi di dati in roaming al dettaglio regolamentati*", la fornitura di servizi di dati in roaming regolamentati ai clienti in roaming direttamente su una rete ospitante da parte di un fornitore alternativo di roaming;

- sostituzione, all'art. 3, del par. 6 con il seguente: "*L'offerta di riferimento di cui al paragrafo 5 è sufficientemente dettagliata e include tutti gli elementi necessari per l'accesso all'ingrosso al roaming di cui al paragrafo 3, fornendo una descrizione delle offerte pertinenti per l'accesso diretto all'ingrosso al roaming e l'accesso alla rivendita all'ingrosso di servizi di roaming, nonché le condizioni correlate. Tale offerta di riferimento può includere condizioni per impedire il roaming permanente o prevenire l'utilizzo anomalo o abusivo dell'accesso all'ingrosso al roaming per scopi diversi dalla fornitura di servizi di roaming regolamentati a clienti dei fornitori di roaming durante i loro viaggi occasionali all'interno dell'Unione. Se necessario, le autorità nazionali di regolamentazione impongono modifiche alle offerte di riferimento per dare effetto agli obblighi previsti dal presente articolo*";
- Modifica del titolo dell'art. 4: "*Vendita separata di servizi di dati in roaming al dettaglio regolamentati*"; soppressione par. 1 co.1, par. 4 e 5;
- Modifica del titolo dell'art. 5: "*Attuazione della vendita separata di servizi di dati in roaming al dettaglio regolamentati*"; modifica del par. 1: *"I fornitori nazionali adempiono l'obbligo relativo alla vendita separata di servizi di dati in roaming al dettaglio regolamentati di cui all'articolo 4 in modo che i clienti in roaming possano utilizzare servizi di dati in roaming separati regolamentati. I fornitori nazionali soddisfano tutte le richieste ragionevoli di accesso alle infrastrutture e ai relativi servizi di sostegno inerenti alla vendita separata di servizi di dati in roaming al dettaglio regolamentati. L'accesso a tali infrastrutture e ai servizi di sostegno che sono necessari per la vendita separata di servizi di dati in roaming al dettaglio regolamentati, inclusi i servizi di autenticazione dell'utente, è gratuito e non comporta oneri diretti a carico dei clienti in roaming*"; modifica del par. 2: *"Per garantire che la vendita separata di servizi di dati in roaming al dettaglio regolamentati sia attuata contemporaneamente e in modo coerente nell'Unione, la Commissione, mediante atti di esecuzione e previa consultazione del BEREC,*

adotta norme di dettaglio relative a una soluzione tecnica per l'attuazione della vendita separata di servizi di dati in roaming al dettaglio regolamentati. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 6, paragrafo 2"; modifica della parte introduttiva del par. 3: "*La soluzione tecnica per l'attuazione della vendita separata di servizi di dati in roaming al dettaglio regolamentati soddisfa i seguenti criteri";*

- Aggiunta dei seguenti articoli:
    - Art. 6-bis: "*abolizione dei sovrapprezzi del roaming al dettaglio*";
    - Art. 6-ter: "*utilizzo corretto"*;
    - Art. 6-quater: "*sostenibilità dell'abolizione dei sovrapprezzi del roaming al dettaglio"*;
    - Art. 6-quinquies: "*attuazione della politica di utilizzo corretto e della sostenibilità dell'abolizione dei sovrapprezzi del roaming al dettaglio"*;
    - Art. 6-sexies: "*fornitura dei servizi di roaming al dettaglio regolamentati"*;
    - Art. 6-septies "*sovrapprezzi transitori del roaming al dettaglio".*

Soffermandoci, infine, sulla modifica della Direttiva n. 2002/22/CE[80], in base a quanto stabilito dal testo del Regolamento n.2120/2015, tale rettifica riguarda il par. 3 dell'art 1, sostituito dal seguente[81]:

"*le misure nazionali in materia di accesso o di uso dei servizi e applicazioni, attraverso reti di comunicazione elettronica, da parte di utenti finali, rispettano i diritti e le libertà fondamentali delle persone fisiche, anche in relazione alla vita privata, e all'equo processo, come definiti dall'art. 6 della Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*".

Attraverso questa modifica si assiste, quindi, ad un sensibile incremento nella tutela dei diritti e delle libertà fondamentali degli utenti finali, ossia coloro che interagiscono ogni giorno nelle fattispecie disciplinate dal Regolamento n.2120/2015 e che necessitano misure nazionali accurate in materia di accesso o di uso dei servizi attraverso le reti di comunicazione elettronica. Il Regolamento sulla Net Neutrality, in conclusione, è entrato in

[80] La Direttiva n 2002/22/CE è una direttiva emanata dal Parlamento Europeo e dal Consiglio, relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica.
[81] Art. 8 Regolamento 2120/2015: "modifica della Direttiva 2002/22/CE";

vigore all'interno dell'UE il 25 novembre 2015 ed ha avuto un impatto significativo nei confronti degli stati membri.

3.2) DSM Strategy

La DSM Strategy, acronimo di Digital Single Market Strategy, è una politica strategica adottata dall'Unione Europea e dagli Stati Membri a partire dal 2015.
L'obiettivo principale che si intende perseguire attraverso tale strategia è quello di garantire all'economia, all'industria e all'intera società economica Europea, la possibilità di trarre il massimo vantaggio e i massimi benefici dalla nuova era digitale.
La DSM Strategy si basa sui seguenti principi:

1. Garantire ai consumatori e alle imprese un miglior accesso ai beni digitali e ai servizi della DSM Strategy;
2. Garantire le giuste condizioni e un campo di sperimentazione e attuazione adatto per i digital networks e per le scienze innovative;
3. Massimizzare il potenziale di crescita dell'economia digitale.

La strategia del mercato unico digitale inizia a riportare i primi risultati positivi già nel 2017, anno durante il quale sono stati raggiunti i seguenti obiettivi:

- Abolizione delle tariffe di roaming [82];
- Modernizzazione della protezione dei dati;
- Portabilità transfrontaliera dei contenuti online;
- Abbattimento delle barriere geo-politiche che ostacolavano l'E-commerce.

La creazione di un mercato unico digitale che va ad operare all'interno dell'Unione Europea rappresenta da sempre una grande possibilità, sia per il raggiungimento di un'innovazione notevole nel campo digitale, sia da un punto di vista economico [83].

[82] vedere paragrafo precedente 3.1 "Regolamento 210/2015 sulla Net Neutrality".
[83] si è stimato infatti che l'adozione di una strategia che fosse finalizzata ad abbattere le barriere geopolitiche del mercato Europeo avrebbe generato un incremento del Pil Europeo di circa quarantacinque miliardi di euro. Molto importanti a riguardo sono state le parole dell'ex Presidente della Commissione Europea Jeanne Claire Junker, in carica dal 2015 al 2019. L'ex Presidente ha sostenuto che fosse molto importante la realizzazione di un progetto simile, poiché ciò avrebbe portato sicuramente ad un miglioramento significativo dei servizi e ad una crescita economica dell'UE di circa duecentocinquanta miliardi di euro, generando conseguentemente migliaia di opportunità e nuovi posti di lavoro per i giovani.

Il problema principale che, secondo la Commissione Europea, ha sempre afflitto il sistema dell'UE è rappresentato dal fatto che i consumatori e le piccole imprese non sono capaci di sfruttare al meglio il commercio elettronico transfrontaliero, vista anche la complessità e la scarsa chiarezza delle norme che disciplinano il settore.

Ciò che rappresenterebbe quindi una soluzione al problema in questione è l'adozione di norme semplificate e moderne che regolamentino gli acquisti transfrontalieri online e digitali, così da incoraggiare le imprese europee ad effettuare vendite online oltre frontiera.

La Commissione Europea sostiene quindi che per raggiungere un traguardo prosperoso ed epocale per la nostra società si deve prima di tutto procedere all'adozione di un quadro regolatorio più semplice, dotato di norme comuni in materia di politica transfrontaliera, per poi procedere conseguentemente alla rimozione dei geo-blocchi ingiustificati che impediscono al consumatore di accedere o di compiere operazioni su portali web che hanno sede in altri Stati.

Naturalmente lo sviluppo di un mercato unico digitale è la chiave della strategia in questione, ma per il suo raggiungimento sono necessari due elementi:

- La volontà politica comune dell'UE e degli Stati membri;
- I mezzi atti a concretizzare tali scopi, quali ad es. fondi, risorse ecc…

Questo porterebbe conseguentemente alla creazione di un clima propizio agli investimenti nelle reti digitali, nella ricerca e nell'imprenditoria innovativa.

Un elemento fondamentale per la DSM Strategy e per la creazione di un mercato unico digitale che operi in tutta l'Unione Europea, è rappresentato dalle piattaforme digitali.

La piattaforma digitale può essere definita come segue: "*uno spazio online utilizzato dagli utenti, con lo scopo di interagire tra loro, sia per finalità commerciali che per altro* [84]".

Le piattaforme in questione consentono la connessione tra gli utenti collegati ad internet, garantendo loro la possibilità di accedere, trasmettere, condividere e commerciare beni o servizi.

Molto interessante è anche la definizione riportata dall'Autorità Tedesca Antitrust, la Bundeskartellamt, la quale ha identificato quattro differenti categorie di piattaforme digitali, le seguenti:

1. Matching platforms, ossia quelle piattaforme, organizzate in maniera bilaterale, che danno la possibilità a due o più gruppi di utenti di interconnettersi tra loro;

[84] T.Gillespie: "the politics of platforms", 2010, Vol. 12, pp 347-364

2. Transaction platforms, cioè quelle utilizzate per determinate tipologie di transazioni, come prenotazioni online di hotel o di appartamenti;
3. Non-transaction platforms, le quali invece garantiscono la possibilità agli utenti di contattarsi privatamente, come ad esempio nei siti di incontri;
4. Audience providing platforms, di tipo unilaterale, dove solo una parte è in grado di beneficiare della crescita del numero degli utenti, e che danno la possibilità ad un gruppo di utenti di essere "osservati", per così dire, da un altro gruppo.

Anche la Commissione Europea nel 2015 ha dato una sua interpretazione al fenomeno delle piattaforme digitali, definendole come segue: "*imprese che operano in mercati a due (o molteplici) facce e che utilizzano Internet per consentire interazioni tra due o più gruppi di utenti distinti ma interdipendenti in modo da generare valore per almeno uno dei gruppi* [85]".
La Commissione ha poi fornito, nella stessa Comunicazione, un elenco di caratteristiche che accomunano le piattaforme digitali, quali:

- la capacità di facilitare ed estrarre valore da connessioni dirette o da interazioni tra utenti;
- La capacità di collezionare, utilizzare e processare una grande quantità di dati personali e non personali;
- Capacità di costruire networks;
- Capacità di creare nuovi mercati.

Tornando alla DSM Strategy e collegandoci alla figura del Provider, si può notare come nell'art. 17 della Direttiva DSM 790/2019 si parli di "OCSSP's", ossia gli "online content sharing service providers"; a riguardo la normativa in questione stabilisce quanto segue: *"Il prestatore di servizi di condivisione di contenuti online effettua un atto di comunicazione al pubblico […] quando concede l'accesso al pubblico a opere protette dal diritto d'autore o altri materiali caricati dai suoi utenti* [86]".

[85]Commissione Europea, COM/2016/288/final.
[86] Art. 17 co.1 Direttiva n. 790/2019 del Parlamento e del Consiglio Europeo.

Secondo la Normativa in questione[87]: "*il prestatore di servizi di condivisione di contenuti online deve pertanto ottenere un'autorizzazione dai titolari dei diritti, ad esempio attraverso un accordo di licenza, al fine di comunicare al pubblico o rendere disponibili al pubblico opere o altri materiali.*

Quando il prestatore di servizi di condivisione online effettui un atto di comunicazione al pubblico o un atto di messa a disposizione del pubblico alle condizioni stabilite dalla presente direttiva, la limitazione di responsabilità di cui all'art. 14, par. 1, Dir. 2000/31/CE[88], non si applica alle fattispecie contemplate dal presente articolo.

Qualora non sia concessa alcuna autorizzazione, i prestatori di servizi di condivisione di contenuti online sono responsabili per atti non autorizzati di comunicazione al pubblico, compresa la messa a disposizione del pubblico, di opere e altri materiali protetti da diritto d'autore, a meno che non dimostrino di:

a) *Aver compiuto i massimi sforzi per ottenere un'autorizzazione;*
b) *Aver compiuto secondo elevati standard di diligenza professionale di settore, i massimi sforzi per assicurare che non siano disponibili opere o altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti;*
c) *Aver agito tempestivamente dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento in futuro, conformemente alla lett.b)".*

La novità introdotta con l'art. 17, si basa sul fatto che i fornitori di servizi di condivisione online dei contenuti, mediante la messa a disposizione del loro servizio agli utenti che caricano contenuti protetti dal diritto d'autore, vanno a compiere essi stessi un vero e proprio atto di comunicazione al pubblico, riservato al titolare dei diritti.

---

[87] Art. 17 co. 2,3 e 4 Dir. n. 790/2019 del Parlamento e del Consiglio Europeo;

[88] Art. 14 par. 1 Dir. 31/2000/CE: "Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

- non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendano manifesta l'illegalità dell'attività o dell'informazione;
- oppure, non appena al corrente dei fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso;

In base all'art. 17 i gestori delle piattaforme, come affermato precedentemente, devono necessariamente richiedere l'autorizzazione al titolare dei diritti per la condivisione di opere protette; se tale autorizzazione non venisse concessa, allora i Providers verrebbero considerati come diretti responsabili della violazione in questione.

Naturalmente la difficoltà nello svolgere operazioni di controllo di ogni singolo upload non è poca, vista l'impossibilità per un singolo o più operatori umani di poter prendere visione e controllare ogni contenuto. In ogni caso l'art. 17 in questione non va ad imporre alcun obbligo generale di sorveglianza [89].

Un'interpretazione simile è stata data dalla Corte di Giustizia dell'Unione Europea nel caso "*Sabam v. Netlog*[90]*",* nel 2010; secondo l'orientamento della Corte, la predisposizione di un sistema di filtraggio, che preveda una sorveglianza generale su tutti i contenuti e file memorizzati dagli utenti presso il gestore della rete sociale, deve essere considerata come qualcosa di inaccettabile, capace di violare alcuni diritti e libertà fondamentali del gestore e degli utenti stessi.

La CGUE, quindi, ha dichiarato che se venisse applicato un sistema di filtraggio, come quello sopra menzionato, si rischierebbe di ledere la libertà di informazione generale, in

[89]Ovviamente non sono mancate critiche e considerazioni nei confronti di questo approccio, una tra le quali è quella avanzata dalla Repubblica di Polonia. Il Governo polacco ha ritenuto che, attraverso l'adozione di un approccio tale, l'UE avesse commesso una violazione del diritto di libertà di espressione e di informazioni, sancito dall'art. 11 della Carta di Nizza.

La Polonia ha sostenuto poi, nella Causa C-401/2019 Corte Europea, Grande Sezione, che le piattaforme, per poter essere esonerate da qualsiasi regime di responsabilità, sarebbero obbligate ad eseguire una sorveglianza preventiva di tutti i contenuti che gli utenti intendono caricare, meccanismo che come menzionato prima risulterebbe quasi impossibile per gli operatori umani.

Quindi la Polonia ha affermato che attraverso tale approccio, l'UE ha effettivamente imposto delle misure di sorveglianza preventiva e generalizzata, senza disporre alcuna garanzia per il rispetto dell'art. 11 della Carta di Nizza.

Al contrario, la Corte ha sostenuto che tale limitazione, anche se sussistente, fosse effettivamente giustificata dal fatto che si intende tutelare anche il diritto d'autore quale diritto fondamentale.

Quindi la Corte ha preferito adottare un orientamento basato sul lasciare ai soggetti onerati la possibilità di scegliere di adottare misure diverse a seconda del caso, con il fine di raggiungere lo scopo perseguito.

Molto interessanti sono state anche le parole dell'Avv. Gen. Henrik Saugmandsgaard ØE, il quale ha stabilito che l'art. 17 della Direttiva DSM è legittimo per ben 3 motivi, quali:

- il fatto che tale articolo ribadisce che non vi sia un obbligo generale di sorveglianza;
- perché il legislatore ha garantito alcune eccezioni e limiti del diritto d'autore che costituiscono esempi di prevalenza dei diritti dei singoli utenti nei confronti dei titolari dei diritti;
- perché le piattaforme digitali devono rimuovere i contenuti palesemente illeciti o simili ad essi.

[90] C-360/10 CGUE, Sez. III;

quanto tale sistema potrebbe non essere in grado di distinguere un contenuto lecito da uno illecito, causando conseguentemente il probabile blocco di contenuti leciti.
In conclusione, anche qui si conferma quanto affermato precedentemente, ossia che l'art. 17 Dir. 790/2019 non impone al prestatore alcun obbligo generale di sorveglianza.

3.2.1) Digital Service Act.

Il Digital Service Act, ossia il Regolamento (UE) 2022/2065 relativo a un mercato unico di dei servizi digitali e che modifica la Direttiva 2000/31/CE, conosciuto con l'acronimo "DSA", è la nuova legge sui servizi digitali approvata nel 19 ottobre 2022 e che entrerà in vigore il 17 febbraio 2024.
Il DSA rappresenta il prototipo di una nuova Costituzione digitale dell'Unione Europea, la quale ha come obiettivi quelli di rafforzare la protezione dei diritti degli utenti e di creare un ambiente digitale più sicuro.
Il DSA. estende la sua regolamentazione a tutto il mercato unico digitale Europeo, anche nei confronti degli operatori di servizi di linea che hanno la propria sede al di fuori dell'UE ma che operano e offrono i loro servizi nel mercato unico digitale.
L'idea che è alla base di questo progetto normativo è quella di disciplinare il mercato unico digitale ad un livello elevato di complessità, cercando di anticipare gli altri legislatori mondiali; si cerca di produrre il c.d. "Brussels effect [91]", un fenomeno che si verifica quando una normativa Europea si pone al vertice della legislazione mondiale in materia, fornendo degli standard a livello globale.
Il DSA, insieme al Digital Market Act (di cui si dirà al paragrafo successivo), va a comporre il c.d. "digital service package", un pacchetto normativo creato con lo scopo di regolamentare lo spazio digitale, definendo misure per la protezione degli utenti online e sostenendo l'innovazione [92].

[91] Il Brussels Effect è un fenomeno in base al quale l'Unione Europea ha la capacità di regolare unilateralmente i mercati globali, ponendosi come punto di riferimento per la regolazione dell'economia digitale e per le sfide per gli Stati Membri.
Questo fenomeno è spesso agevolato dal fatto che le Multinazionale preferiscono utilizzare un tipo di politica conforme e unitaria, finendo così ad estendere molte volte le politiche dell'Unione Europea a tutte le proprie attività intorno al mondo, evitando il disturbo e il costo di doversi adeguare ad una moltitudine di sistemi diversi;
[92] Tale pacchetto normativo è stato definito dalla Presidente della Commissione Europea Ursula Von Der Leyen come un accordo storico, sia in termini di rapidità che di sostanza;

L'obiettivo che sta alla base del DSA e di tutto il digital service package è principalmente quello di creare uno spazio digitale aperto e più sicuro, fondato sul rispetto dei diritti fondamentali.

A riguardo, la normativa in questione va a suddividere le piattaforme intermediarie di servizi in quattro categorie:

a) *servizi di hosting*, come i servizi di cloud storage, ossia risorse elettroniche presenti su internet che forniscono agli abbonati la possibilità di sfruttare potenti risorse di memorizzazione online senza dover acquistare o utilizzare hardware e software;
b) *Piattaforme online*, che hanno la capacità di mettere insieme e connettere venditori e consumatori, come ad esempio i social media e gli app. Stores;
c) *Servizi intermediari*, i quali possono essere definiti come: "*le piattaforme che consentono agli utenti commerciali di offrire beni e servizi avendo quale obbiettivo quello di facilitare l'avvio della transazione diretta con i consumatori* [93]";
d) *Very large online platforms*. Queste piattaforme sono conosciute anche con l'acronimo di VLOP's e vengono definite dal DSA come quelle piattaforme online in cui il numero di utenti mensili è pari o superiore al 10% totale dei consumatori dell'UE, come ad esempio Alibaba o Amazon. Si tratta di piattaforme che, per via della loro grandezza ed estensione, sono esposte ad un maggior numero di rischi, come ad es. la disseminazione di materiale illecito, ed è per questo che necessitano una maggiore attenzione da parte della Commissione Europea.

Da un punto di vista più strutturale, il DSA si suddivide nelle seguenti 3 aree tematiche di intervento:

- Disciplina della responsabilità degli intermediari o anche dell'esenzione di tale responsabilità, in cui vengono ripresi alcuni dei concetti della Dir. n. 2000/31, apportandovi aggiornamenti e modifiche;
- Obblighi di dirigenza degli intermediari;
- Definizione del ruolo delle autorità di vigilanza come "coordinatori" dei poteri della Commissione Europea, con conseguente individuazione dei parametri sanzionati.

[93] BLB Studio Legale, servizi di intermediazione online, blblex.it, 2020

Attraverso il DSA vengono stabilite anche delle misure atte a contrastare la diffusione, nelle piattaforme digitali, di contenuti, beni e servizi considerati come illeciti; vengono definite inoltre anche delle nuove regole per il tracciamento dei venditori sui mercati online, ponendo degli obblighi di verifica della sicurezza e della liceità dei beni e servizi da loro offerti.

Critiche e discussioni sul DSA

La questione posta al centro di numerose discussioni tra alcune "*Big tech*[94]" Europee come Zalando o Amazon, riguarda il rischio che il D.S.A. possa in realtà causare una brusca frenata per i giganti del web e non una rivoluzione normativa digitale, come previsto.

La critica di maggior spessore è stata avanzata dalla famosa Compagnia operante nel settore dell'abbigliamento, Zalando, la quale ha avanzato nel 17 giugno 2023 un'azione legale presso la Corte di Giustizia dell'Unione Europea, facendo riferimento all'art. 33 del Regolamento (UE) n. 2022/2065 e contestando la denominazione di "very large online platform", attribuitagli dal DSA, che, secondo la compagnia tedesca, provocherebbe una censura nei loro confronti.

Zalando si è opposta all'adozione di tale normativa, facendo ricorso alla CGUE, sostenendo che la loro presenza nella "*lista dei 19* [95]" fosse ingiustificata, vista la mancanza dei requisiti e delle caratteristiche che la qualificherebbero come un social network e come una VLOP.

Zalando inoltre contestava il mancato inserimento in questa lista di piattaforme come ad es. Netflix.

Le critiche avanzate da Zalando sono, quindi, tutte incentrate su uno scetticismo generale nei confronti dell'UE, la quale, secondo tali orientamenti, andrebbe ad assumere un potere di limitazione e di censura nei confronti della piattaforma.

[94] Per Big tech si intendono le aziende leader nel loro settore informatico e digitale, che hanno un notevole potere economico e influenza sulla società e sull'economia globale.

[95] La lista dei 19 è un elenco redatto dalla Commissione Europea all'interno del quale vengono citate tutte le Very Large Online Platforms, anche conosciute con l'acronimo VLOP's, le quali devono necessariamente sottoporre le loro politiche interne alle misure e alle limitazioni indicate nel Digital Service Act.

Il Commissario Europeo al Mercato Interno e all'Industria, Thierry Breton, è intervenuto sul caso, sostenendo quanto segue [96]: "*in Europa non ci sarà il Ministero della Verità; ciò che ci sarà è trasparenza, nei processi algoritmici, nei bot e negli annunci personalizzati*". Continua poi: "*io e i miei servizi applicheremo scrupolosamente il DSA, utilizzeremo personalmente i nostri nuovi poteri sulle piattaforme e sanzioneremo ove necessario. Rispettare il DSA non è una punizione ma un'opportunità per le piattaforme di rafforzare la propria affidabilità*".

Gli aspetti della normativa che sono stati maggiormente criticati sono i seguenti:

- la piattaforma deve mettere in atto un sistema di ricorso e. l'authority nazionale (Agcom nel caso dell'Italia), se necessario, deciderà in ultima istanza. Se il ricorso verrà accolto, la piattaforma dovrà ripristinare il contenuto e pagare i costi;
- Le aziende dovranno dare spiegazioni sul perché consigliano contenuti agli utenti in base al loro profilo, specificando in maniera dettagliata tutte le informazioni inerenti a tale processo;
- Le aziende dovranno anche redigere dei rapporti annuali per consentire all'autorità di verificare il rispetto dei requisiti.

In caso di violazione di queste disposizioni sono previste pesanti sanzioni che arrivano fino al 6% del fatturato globale dell'azienda nell'esercizio annuale, con ulteriore possibilità di messa al bando in caso di recidiva.

Sono state molte quindi le critiche e le osservazioni avanzate, specialmente dalle Big Tech, nei confronti di questa nuova normativa, ma allo stesso tempo ci sono state anche alcune compagnie appartenenti alla "*lista dei 19"* le quali hanno subito attivato processi di adattamento delle loro politiche interne alle disposizioni del D.S.A.

[96] D. Aliperto: Digital Services Act, Breton: "Non è ministero della Verità ma chance per le Big tech", Corcom, 2023.

L'esempio maggiormente rappresentativo è quello di Google, i cui vertici, fin da subito, hanno rilasciato dichiarazioni riguardo l'adattamento futuro di molti dei loro processi di sicurezza e di fiducia, alle nuove regole imposte dalla riforma [97].

Tornando alle modifiche introdotte dal DSA, possiamo osservare come la normativa in questione abbia apportato due novità molto importanti, le seguenti:

1. l'adattamento del ruolo dello "Chief Compliance Officer" (C.C.O.) alle politiche interne della normativa. Il Compliance Officer è una figura nata nell'ultimo decennio, precisamente intorno al 2014/2015, in seguito a determinati scandali economici e commerciali avvenuti in Europa (come lo scandalo ADAC-Volkswagen[98]), che hanno portato alla nascita di normative e regole più stringenti nei confronti delle aziende e delle loro politiche interne.

   L'obiettivo principale, quindi, è quello di far fronte all'aumento normativo e dei controlli nei confronti delle aziende e delle loro politiche interne. Lo C.C.O. ha lo scopo di garantire che l'azienda da esso rappresentata agisca in conformità delle norme applicabili.

   Il ruolo del C.C.O. è esteso anche ad altri settori, quali ad es:

   - il monitoraggio delle VLOPs, con il fine di verificare il rispetto e la compatibilità di queste piattaforme con le politiche dettate dal D.S.A.;
   - la cooperazione e il collegamento con le autorità competenti quando richiesto.
   - la gestione di situazioni di crisi d'impresa, in base a quanto stabilito dall'art. 2086 c.c.[99]

[97] Ci sono poi stati anche i casi di Meta e Tiktok, che, in risposta alle condizioni dettate dal DSA, hanno provveduto ad apportare alcune modifiche interne e a rilasciare alcune dichiarazioni a riguardo. Meta ha rilasciato dichiarazioni riguardo l'aggiornamento dell'AD library, ossia una funzione che consiste nel raccogliere annunci pubblicitari all'interno della piattaforma e che, in ottemperanza al DSA, dovrà fornire l'archiviazione e la visualizzazione di tutti gli annunci che hanno come target utenti cittadini UE. Tiktok, invece, ha rilasciato dichiarazioni riguardo la possibilità di rendere opzionale il suo algoritmo per gli utenti UE, dando l'opportunità a questi di poter accedere a contenuti di tutto il mondo, non basandosi solo sulle loro preferenze personali.

[98] Lo scandalo ADAC-Volkswagen è avvenuto intorno al 2014/15 e ha interessato il club automobilistico tedesco ADAC, con sede a Monaco di Baviera, e il gruppo automobilistico tedesco Volkswagen. Lo scandalo ha riguardato un'operazione fraudolenta da parte del club ADAC, che avrebbe truccato le votazioni inerenti all'auto dell'anno 2014, assegnando il titolo alla Volkswagen Golf;

[99] Art. 2086 c.c. "gestione dell'impresa";

Esistono diverse categorie di Chief Compliance Officer a seconda della materia di riferimento:

- Antitrust; con la pubblicazione da parte dell'AGCM, nel 2014, dello schema delle linee guida sulla compliance antitrust, l'autorità ha definito il complesso di misure e di regole di condotta che devono essere attuate per una effettiva compliance antitrust. Il programma di compliance pubblicato dall'Autorità Antitrust è un complesso di regole aventi sostanzialmente una funzione preventiva di condotte potenzialmente rilevanti in termini di illecito antitrust;
- D.lgs. 231/01 [100], entrato in vigore nel 4 luglio 2001, che introduce il Modello 231; si tratta di una normativa che ha introdotto il principio per cui le società possono essere ritenute responsabili della commissione di reati. Il modello 231 è un programma volto a descrivere una serie di procedure aziendali volte a garantire la prevenzione della commissione di reati. Il modello 231 non è obbligatorio, ma se adottato da un'azienda, prevede la nomina di un ODV, ossia di un organismo di vigilanza, il quale ha il compito di verificare l'efficienza del Modello e della sua effettiva applicazione;
- SDG 16, Sustainable Development Goals [101]; si tratta di un programma avanzato dalle Nazioni Unite nel 2015 con lo scopo di promuovere società pacifiche e inclusive per uno sviluppo sostenibile, garantire l'accesso alla giustizia per tutti e costruire delle istituzioni efficaci e inclusive a tutti i livelli. Secondo le Nazioni Unite il Compliance Officer ha qui un ruolo di rilevante importanza nel raggiungimento di tali obiettivi, promuovendo trasparenza, responsabilità e aderenza alle regole dettate dalla legge. In tal caso quindi i Compliance Officer svolgono un ruolo significativo nella realizzazione del programma "SDG 16", nel rispetto delle regole e nell'intermediazione tra organizzazioni e autorità;

[100] D.lgs. 8 giugno 2001, n.231, disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11, L. 29 settembre 2000, n. 300;
[101] United Nations, Sustainable Development Goals 16, 2015;

2. l'introduzione della figura del "Digital Service Coordinator" (DSC). Si tratta di un'autorità scelta dagli Stati Membri con il fine di garantire il rispetto del nuovo Regolamento. Il DSC ha avuto un impatto significativo, specialmente sul nostro ordinamento; il Presidente dell'Agcom Giacomo Lasorella, nella Presentazione della Relazione Annuale al Parlamento del 2022, ha affermato a riguardo che l'Autorità per le Garanzie sulle Comunicazioni ha tutti i requisiti necessari per essere considerata come il DSC italiano [102]. La figura in questione si caratterizzata per i seguenti aspetti:
    - si occupa della gestione dei ricorsi e dei reclami inviati dagli utenti contro i gestori dei servizi di intermediazione per la violazione degli obblighi imposti dalla legge;
    - porta avanti investigazioni, interviste e ispezioni;
    - è sottoposto alle misure di trasparenza necessarie, come ad esempio la redazione annuale di un registro nel quale sono riportate tutte le sue attività;

    Il DSC inoltre è dotato di alcuni poteri, quali ad esempio[103]:
    - il potere di ordinare la cessazione delle violazioni e, se necessario, il potere di imporre dei rimedi proporzionati a contrastare e porre fine al comportamento illecito;
    - il potere di imporre sanzioni e/o pagamenti periodici;
    - il potere di adottare misure ad interim;
    - Il potere di accettare gli impegni offerti dai providers, in relazione al rispetto del DSA e, di rendere tali impegni vincolanti.

[102] L' Agcom è stata effettivamente nominata "digital service coordinator", con il D.L. n. 2023/123, pubblicato sulla gazzetta ufficiale n.216 del 15 settembre 2023;

[103] anche se il DSC e lo CCO sono due figure diverse che operano in ambiti distaccati, ci sono alcune sovrapposizioni tra le funzioni svolte dai due e i poteri di cui sono dotati, come ad es: coordinazione e gestione di attività specifiche, collaborazione con altri dipartimenti e team tecnici, monitoraggio delle performance, definizione di standard e di sanzioni;

3.2.2) Digital Market Act

Il Digital Market Act, conosciuto anche con l'acronimo "DMA.", è un recente Regolamento (UE) n. 2022/1925, approvato dal Parlamento Europeo il 5 luglio 2022 ed entrato in vigore il 2 maggio 2023, che fa parte del già menzionato digital service package.
Gli obiettivi che si intendono perseguire attraverso il DMA sono i seguenti:

- Garantire l'assenza di barriere all'ingresso di tutti i servizi online;
- Combattere gli abusi di mercato compiuti dalle grandi piattaforme digitali;
- Stimolare l'innovazione e la concorrenza nei mercati digitali;
- Offrire una maggiore possibilità di scelta ai cittadini europei nell'ambito dei servizi digitali;
- Creare uno spazio economico più equo per le imprese europee;
- Favorire la suddivisione di valori e utili tra le imprese che operano nell'economia digitale.

La normativa in questione, tra i vari incarichi, ha lo scopo di identificare quando una piattaforma digitale ha raggiunto una dimensione e un'importanza così elevate, da poter essere considerata come una "gatekeeper".
La traduzione letterale del termine "gatekeeper" è: "guardiani del cancello", interpretazione che non si allontana molto da ciò che si vuole intendere veramente con questo termine. Le piattaforme vengono considerate come gatekeeper quando raggiungono un impatto significativo sul mercato interno, fungendo da gestori dei punti di accesso a dei servizi digitali per utenti e consumatori.
Esistono dei criteri che devono essere rispettati per poter considerare una piattaforma digitale come una gatekeeper:

- Un impatto significativo sul mercato interno, con un fatturato pari o superiore a 7,5 miliardi di euro, negli ultimi tre esercizi, ovvero il valore totale delle azioni corrispondente a 7,5 miliardi di euro nell'ultimo esercizio annuale;
- Il controllo di un importante punto di accesso (gateway) per le aziende sui consumatori finali, con un numero di utenti attivi mensilmente, che ruota intorno ai quarantacinque milioni;
- Una dimensione notevole e una posizione forte e duratura nel tempo;

Il DMA pone, quindi, le basi per contrastare il potere dei gatekeeper, impedendo che gli stessi concretino abusi della loro posizione dominante nel mercato di riferimento [104].
Gli obblighi e le pratiche che devono essere rispettati dai gatekeepers sono regolamentati dal DMA negli artt. 5 e 6:

- Non deve trattare, al fine della fornitura dei servizi pubblicitari online, i dati personali degli utenti servizi di terzi che si avvalgono di servizi di piattaforma di base del gatekeeper
- Non deve combinare dati personali provenienti dal pertinente servizio di piattaforma di base con dati personali provenienti da altri servizi di piattaforma di base o da eventuali ulteriori servizi forniti dal gatekeeper o con dati personali provenienti da servizi di terzi;
- Non deve utilizzare in modo incrociato dati personali provenienti dal pertinente servizio di piattaforma di base in altri servizi forniti separatamente dal gatekeeper, compresi altri servizi di piattaforma di base;
- Deve consentire agli utenti finali di installare app o piattaforme esterne, che garantiscono la connessione con il sistema operativo del gatekeeper;
- Deve consentire agli utenti commerciali di offrire gli stessi prodotti o servizi, attraverso sistemi di intermediazione online di terzi, a prezzi o condizioni più favorevoli o comunque diversi da quelli offerti dai gatekeepers;

[104] Art. 102 TFUE, ex art. 82 TCE, È incompatibile con il mercato interno e vietato, nella misura in cui possa essere pregiudizievole al commercio tra Stati membri, lo sfruttamento abusivo da parte di una o più imprese di una posizione dominante sul mercato interno o su una parte sostanziale di questo. Tali pratiche abusive possono consistere in particolare:

a) nell'imporre direttamente od indirettamente prezzi d'acquisto, di vendita od altre condizioni di transazione non eque;

b) nel limitare la produzione, gli sbocchi o lo sviluppo tecnico, a danno dei consumatori;

c) nell'applicare nei rapporti commerciali con gli altri contraenti condizioni dissimili per prestazioni equivalenti, determinando così per questi ultimi uno svantaggio per la concorrenza;

d) nel subordinare la conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari, che, per loro natura o secondo gli usi commerciali, non abbiano alcun nesso con l'oggetto dei contratti stessi.

- Deve consentire alle aziende/imprese di promuovere le loro offerte e di concludere contratti con i loro clienti, al di fuori della piattaforma del gatekeeper;
- Deve fornire agli utenti commerciali un accesso efficace, di elevata qualità, continuo e in tempo reale, a tutti i dati aggregati e non aggregati.
- Deve astenersi dall'utilizzare, in concorrenza con gli utenti commerciali, dati non accessibili al pubblico, generati attraverso le attività di tali utenti commerciali;
- Deve astenersi dal limitare a livello tecnico la possibilità per gli utenti finali di passare e abbonarsi a servizi e applicazioni diversi;
- Deve astenersi dal garantire un trattamento più favorevole in termini di posizionamento ai servizi e prodotti offerti dal gatekeeper stesso, o da terzi che appartengono alla stessa impresa, rispetto ai servizi o prodotti analoghi di terzi e, applicare condizioni eque e non discriminatorie a tale posizionamento.

Il DMA ha, inoltre, insignito la Commissione Europea di nuovi poteri, quali ad es:

- Il potere di concedere una sospensione di un obbligo del gatekeeper se si verificano determinate condizioni: "*Qualora il gatekeeper dimostri in una richiesta motivata che l'osservanza di un obbligo specifico di cui agli articoli 5, 6 o 7 relativo a un servizio di piattaforma di base elencato nella decisione di designazione a norma dell'articolo 3, paragrafo 9, metterebbe a rischio, a causa di circostanze eccezionali che sfuggono al controllo del gatekeeper, la redditività economica della sua attività nell'Unione, la Commissione può adottare un atto di esecuzione recante la sua decisione di sospendere in via eccezionale, in tutto o in parte, l'obbligo specifico di cui a tale richiesta motivata* [105]"
- il potere di concedere un'esenzione per motivi di interesse pubblico: "*La Commissione, agendo su richiesta motivata di un gatekeeper o di propria iniziativa, può adottare un atto di esecuzione recante la sua decisione di esentare tale gatekeeper, integralmente o in parte, da un obbligo specifico sancito dagli articoli 5, 6 o 7 in relazione a un servizio di piattaforma di base elencato nella decisione di designazione a norma dell'articolo 3, paragrafo 9, se tale esenzione è giustificata in base ai motivi di cui al paragrafo 3 del presente articolo («decisione di*

[105] Art. 9 co. 1 Reg. 2022/1925

esenzione»). La Commissione adotta la decisione di esenzione entro tre mesi dalla ricezione di una richiesta motivata completa e fornisce una dichiarazione motivata che illustra i motivi dell'esenzione [106]".

L'art. 12 della normativa in questione stabilisce un meccanismo per l'aggiornamento dell'elenco degli obblighi basato sui poteri della Commissione.
La Commissione interviene ove si ritenga che una pratica sia sleale o limiti la contendibilità del mercato nei seguenti casi:

- in caso di creazione di uno squilibrio tra diritti ed obblighi per gli utenti commerciali, con la conseguenza che il gatekeeper sia riuscito a trarre un vantaggio altamente sproporzionato dal servizio fornito agli utenti in questione;
- nel caso in cui la contendibilità dei mercati è diminuita in conseguenza di una siffatta pratica adottata da un gatekeeper.

La procedura mediante la quale una piattaforma, gestita da una compagnia, può inoltre essere considerata come "Gatekeeper" è la seguente:

- la compagnia in questione deve innanzitutto rivolgersi alla Commissione Europea, comunicandovi tutti i dati e le informazioni riguardanti la sua posizione sul mercato, il ruolo, il potere o l'influenza che esercita nel settore in cui opera;
- successivamente la Commissione procede ad una valutazione dettagliata delle informazioni fornite dalla compagnia, verificando la loro attendibilità;
- se la Commissione ritiene soddisfacenti e attendibili i dati forniti dalla compagnia, procede con l'assegnazione della norma; se invece accade il contrario, la Commissione darà alla compagnia un termine ultimo di sei mesi entro il quale dovranno essere adattati tutti gli aspetti considerati come non soddisfacenti. Al termine di questo periodo, se le modifiche richieste non sono state applicate dalla compagnia, la Commissione potrà procedere con l'imposizione di sanzioni quali ad es. il pagamento di una somma pari al 10/20 % del fatturato annuale della compagnia, oppure in caso di ripetute violazioni, un pagamento periodico del 5% del fatturato totale giornaliero.

[106] Art. 10 co.1 Reg. 2022/1925;

Infine, nell'art. 17 della normativa, si tratta dell'indagine di mercato per la designazione di gatekeeper: *"la Commissione può procedere ad un'indagine di mercato al fine di valutare l'opportunità di designare un'impresa che fornisce servizi di piattaforma di base come gatekeeper a norma dell'articolo 3, paragrafo 8, o al fine di identificare i servizi di piattaforma di base da elencare nella decisione di designazione a norma dell'articolo 3, paragrafo 9 […] Al fine di concludere la sua indagine di mercato, la Commissione adotta un atto di esecuzione che stabilisce la sua decisione […] Nel corso di un'indagine di mercato a norma del paragrafo 1 del presente articolo, la Commissione si adopera per comunicare le proprie constatazioni preliminari all'impresa che fornisce servizi di piattaforma di base interessata entro sei mesi dalla data di cui all'articolo 16, paragrafo 3, lettera a) […] Se l'impresa che fornisce servizi di piattaforma di base raggiunge le soglie stabilite dall'articolo 3, paragrafo 2, ma ha presentato argomentazioni sufficientemente fondate in conformità dell'articolo 3, paragrafo 5, che hanno messo manifestamente in dubbio la presunzione di cui all'articolo 3, paragrafo 2, la Commissione si adopera per concludere l'indagine di mercato entro cinque mesi dalla data di cui all'articolo 16, paragrafo 3, lettera a)* [107] *".*

Possiamo sostenere quindi che il DMA, insieme al DSA e all'intera DSM strategy, rappresenta un nuovo modo di regolamentare il mercato digitale europeo, una nuova frontiera del commercio digitale, volta a ridurre al minimo ogni forma di corruzione, ostacolo e abuso all'interno del mercato.

Ci sono, tuttavia, alcuni punti della normativa in questione che sono stati messi in discussione dalla Dottrina a causa di una scarsa precisione e di una poca chiarezza:[108] "*la concezione di gatekeeper, espressa dall'art. 3 DMA, manca di una chiara specificazione riguardo la soglia di potere rilevante. Secondo quanto espresso dall'European Commission Impact Assesment, la soglia quantitativa stabilita nell'art. 3 co.2 dovrebbe includere 10 fornitori di servizi delle piattaforme principali. Inoltre, è stato suggerito che il DMA dovrebbe garantire un maggior grado di flessibilità nell'adattare le regole ai rischi competitivi associati a servizi e modelli di business specifici. È stato poi puntualizzato che la normativa dovrebbe incoraggiare esplicitamente l'applicazione da parte dei privati e*

[107] Art. 17 Reg. 2022/1925;

[108] G. Muscolo, "the Digital Market Act and the asymmetric regulation for platforms", Ius.giuffrefl.it, 2022;

conferire alle autorità nazionali il potere di impegnarsi in un'applicazione decentralizzata delle regole di condotta imposte ai gatekeeper, accompagnata da forti meccanismi di coordinamento per garantire un'adeguata assegnazione dei casi e un'interpretazione coerente delle regole. Oltretutto è stato poi segnalato come il controllo delle fusioni dei mercati controllati dai gatekeepers rimanga una lacuna. Sebbene l'attenzione della DMA alle regole di condotta sia giusta, dovrebbe probabilmente essere integrata da una speciale revisione preventiva delle acquisizioni dei gatekeeper".

Le questioni che sono state avanzate sono le seguenti:

- *"la DMA sostituirà in gran parte l'applicazione dell'art. 102 TFUE?*
- *Oppure costituirà uno stimolo per ripensare le metodologie del diritto della concorrenza dell'UE, ad esempio per quanto riguarda la definizione del mercato e la direzione che il diritto della concorrenza dell'UE ha preso nell'ultimo decennio?"*

In conclusione, quindi, la normativa DMA cambierà sicuramente la realtà giuridica per i gatekeepers. "*Il Regolamento in questione è ispirato al diritto della concorrenza e porterà per sempre con sé questo carattere; allo stesso tempo è importante ricordare che il DMA si differenzia da questa branca del diritto sotto diversi aspetti: segue un sistema di divieto, contiene un numerus clausus di obblighi prescrittivi e divieti, ed è un regime di regolamentazione settoriale ex-ante. La sfida consisterà nel capire come garantire che la complementarità tra la DMA e le regole della concorrenza non si traduca in frammentazioni e incoerenze* [109]".

3.3) Dibattito sul Fair Share.

Il Fair Share è un progetto sviluppato dall'Unione Europea in epoca molto recente, precisamente nel giugno 2023, in seguito alla votazione del Parlamento Europeo, il quale si è espresso in maggioranza a sostegno del principio "senders pay".
La riforma "fair share", che tradotto sta per "giusta quota", mira a regolamentare i costi d'investimento nelle reti di telecomunicazione, introducendo per legge una condivisione dei costi.

[109] A.P. Komminos, "The Digital Markets Act How does it compare with competition law", ius.giuffrefl.it, 2022;

Il principio in questione nasce con lo scopo di istituire un quadro politico Europeo nel quale i grandi generatori di traffico contribuiscano equamente al finanziamento adeguato delle reti di telecomunicazione, fatta salva la neutralità della rete.

Quindi, con tale iniziativa, si intende sostenere che un'elevata percentuale del traffico in rete viene generato dalle Big Tech del settore, le quali, conseguentemente, raccolgono la maggior parte dei benefici dell'economia di internet, senza però poi pagare i costi delle reti che trasportano quel traffico.

La proposta del Fair share è stata si avanzata in epoca molto recente all'interno dell'Unione Europea, ma ha delle origini ben più lontane, infatti risale precisamente al 2012 [110], anno in cui si è sviluppato un intenso dibattito tra alcuni grandi Telco europee che fanno parte delle associazioni di ETNO[111] e GSMA[112], secondo le quali: "*le maggiori piattaforme online americane dovrebbero pagare per il trasporto dei rispettivi servizi attraverso le reti europee di telecomunicazioni che le connettono agli utenti* [113]".

Come citato precedentemente, il principio sostenuto dalle Telco è quello del "Senders Pay" o "Senders Party Network Pays", un meccanismo secondo il quale la rete da cui si spedisce del traffico internet deve pagare quella di destinazione, esattamente come accadeva in passato con le telefonate analogiche tradizionali.

Il perno di questa riforma consiste quindi in un meccanismo di tariffazione del traffico internet che porterebbe i maggiori operatori globali (BigTech) a pagare agli operatori di telecomunicazioni (Telco) una tassa per il passaggio dei servizi di internet sulle loro reti.

Il meccanismo di tariffazione in questione costituirebbe quindi:

- una giusta remunerazione per l'utilizzo delle reti delle Telco da parte degli operatori internet che le sfruttano per vendere i propri servizi agli utenti;
- un finanziamento dello sviluppo delle reti ad alta velocità necessarie per sostenere il costante incremento del traffico internet (5G e fibra ottica).

---

[110] I. Genna; Fair Share, "come Bruxelles potrebbe riscrivere le regole di internet", 2023, par. 1;

[111] European Telecommunications Network Operators' Association; si tratta del principale gruppo politico europeo che si occupa della gestione delle reti di telecomunicazioni. Fondato nel 1992 e composto da 38 membri, l'ETNO riunisce i principali investitori in piattaforme e servizi di comunicazione elettronica innovativi e di alta qualità, che rappresentano il 70 % degli investimenti totali del settore;

[112] Global System for Mobile Association; si tratta di un'associazione europea, fondata nel 1982, con lo scopo di semplificare la collaborazione e garantire l'interoperabilità tra coloro che utilizzano le tecnologie GSM;

[113] vedi nota 110;

Il principio del Fair Share è sempre stato sostenuto dal Commissario per il Mercato Interno Thierry Breton, il quale ha sostenuto che: "*internet ad alta velocità richiede investimenti elevati. Ecco perché, oltre a facilitare l'implementazione della rete a breve termine, stiamo esplorando l'importante questione di chi dovrebbe pagare per la prossima generazione di infrastrutture di connettività* [114]". Ha continuato poi sostenendo quanto segue: "*Il divario di investimenti più ottimistico entro il 2030 ruota intorno a centosettantacinque miliardi di euro per gli operatori di telecomunicazioni*".

La Commissione Europea, con lo scopo di valutare gli investimenti effettuati dalle società di telecomunicazione (TELCO) e quelle delle società c.d. "*over the top* [115]" (OTT), nel campo delle reti e dei cloud e delle tecnologie emergenti, ha preparato un apposito questionario, composto da sessantadue domande, divise in quattro temi principali, i seguenti:

- investimenti su reti, cloud e tecnologie emergenti, nel quale viene richiesto alle Telco e alle Ott di fornire informazioni sulle loro strategie di investimento, comprese le fonti di finanziamento e le tecnologie su cui si concentrano; gli operatori devono poi fornire informazioni sulle iniziative che stanno intraprendendo per migliorare l'efficienza delle reti, la sicurezza e la protezione dei dati e per sviluppare nuovi servizi e modelli di business;
- Equità per i consumatori, dove viene richiesto alle Telco e alle Ott di fornire informazioni sulle politiche di gestione del traffico, in particolare sull'assegnazione della priorità del traffico e sulla gestione della congestione. Devono essere fornite anche le misure adottate per garantire l'accesso a internet a tutti i consumatori;
- Ostacoli al mercato unico, in cui si ha lo scopo di eliminare le barriere all'accesso e alla competizione nei servizi di comunicazione elettronica tra gli stati membri dell'UE. Devono essere fornite dall'UE le informazioni sulle difficoltà incontrate nell'offerta di servizi transfrontalieri e sulle azioni intraprese per affrontare tali problematiche;

[114] F. Meta, "Butti all'UE, rinviare la proposta in attesa di dati certi", Corcom, 2023;

[115] Per Ott, ossia "over the top", si intendono secondo quelle società e/o imprese che forniscono, attraverso la rete Internet, servizi, video e pubblicità mentre si naviga online, Esse traggono ricavo, in prevalenza, dalla vendita di contenuti e servizi tramite concessionari agli utenti finali o di spazi pubblicitari, come nel caso di Google e Facebook. Gli utenti possono accedere ai contenuti tramite qualsiasi tipo di unità con una connessione a banda larga.

- Contributo equo a tutti gli attori digitali, capitolo che rappresenta il cuore del questionario, nel quale viene chiesto agli operatori di specificare la soglia di considerazione di un'azienda come un generatore di traffico. Si chiede poi di quantificare gli investimenti per le infrastrutture digitali e di rete in grado di ottimizzare il traffico di rete e, infine, di determinare quali potrebbero essere gli effetti di un meccanismo che obblighi i granfi generatori di traffico a contribuire allo sviluppo della rete e ad avere obblighi sull'impronta ambientale dei servizi forniti dalle reti.

Analizzando in modo più approfondito la teoria del fair share, sono emersi molti dubbi e incongruenze con il sistema commerciale al quale questo progetto dovrebbe essere applicato, non a caso infatti sia la comunità tecnica internet che l'agenzia europea BEREC[116], si sono espresse con scetticismo nei confronti dell'adozione del principio sin qui trattato[117].

La strategia in questione presenta alcuni punti critici e problematiche non di poco conto, ma anche alcuni benefici ed aspetti postivi:

- Prima di tutto occorre chiederci chi è che paga effettivamente per il trasporto dei servizi agli utenti. Secondo quanto espresso dall'ex parlamentare danese Frode Sorensen [118] sono gli utenti stessi i diretti interessati, coloro che pagano per il trasporto dei servizi di internet; non sono quindi gli OTT a sfruttare le reti di telecomunicazione, semmai sono le Telco a fornire tali reti ai propri utenti per accedere ai servizi internet che preferiscono. Gli utenti pagano tale servizio di trasporto alle Telco attraverso l'abbonamento di internet; quindi, l'idea di far pagare gli OTT per lo sfruttamento delle reti di telecomunicazione, porterebbe ad un doppio pagamento del medesimo servizio di trasporto, prima alle società over the top e poi agli utenti;
- Si potrebbe, inoltre, generare un problema di concorrenza tra Telco e Ott, precisamente con riferimento al momento dell'interconnessione tra le due e alla negoziazione del prezzo di consegna del traffico IP. Alcune società di

[116] Berec: organismo dei regolatori europei delle comunicazioni elettroniche, fondato nel 2009 e con sede a Riga;
[117] J. Hoffman; "29 Internet experts and academics send a letter to the Commission urging to abandon the sending party network pays proposal", 2022, www.komaitis.org;
[118] F. Sorensen, "2022 Fair Share discussion and 2012 BEREC statement to ITU/WCIT", Nkom, 2022;

telecomunicazione[119] sostengono di non poter rifiutare l'interconnessione, e quindi, sarebbero conseguentemente costrette ad interconnettersi, anche gratuitamente, a causa delle regole di net neutrality. In realtà tale affermazione è falsa, poiché, secondo quanto espresso dalla Dir. n. 97/33/CE del Parlamento Europeo e del Consiglio [120], gli operatori sono liberi di rifiutare l'interconnessione per motivi commerciali, a meno che siano dominanti, in quanto: "*la necessità di mantenere l'integrità della rete non rappresenta una giustificazione valida per rifiutare di negoziare le condizioni di interconnessione*".

Nei mercati dell'interconnessione IP quindi non si prevede che una delle parti possa addebitare all'altra i costi di trasporto sulla propria rete, ma non vi è in realtà neanche una regola che lo proibisca.

Le discussioni e le problematiche inerenti alla tematica del Fair share sono state quindi molte e ripetute e, vista la delicatezza della questione, si è assistito anche ad un leggero passo indietro da parte della Commissione Europea [121]

L'imposizione del pagamento di una tassa per gli OTT andrebbe a sconvolgere il mercato Europeo, poiché le società over the top potrebbero scegliere di non consegnare più i loro servizi all'interno dell'UE e rivolgere la loro attenzione altrove, con la conseguenza che i servizi di telecomunicazione europei diminuirebbero si sicurezza e qualità.

In conclusione quindi, con riferimento al Fair Share, ci troviamo dinanzi ad una situazione abbastanza delicata e complessa, la quale necessita di essere interpretata in maniera corretta e con un approccio adeguato a poter condurre l'Unione Europea al raggiungimento di numerosi benefici e vantaggi.

[119] G. Ponte; G. Robustelli, "si scrive Fair share, si legge Fair play", Tim, 2023;

[120] Art. 10 co.1 Lett. b) Dir. n. 97/33/CE del Parlamento Europeo e del Consiglio sull'interconnessione nel settore delle telecomunicazioni e finalizzato a garantire il servizio universale e l'interoperatività attraverso l'applicazione dei principi di fornitura di una rete aperta (ONP);

[121] nell'ottobre 2023, Breton ha sostenuto la necessità di adottare un Digital Network act, ossia una normativa che si aggiunge alla strategia del Fair share per trovare un modello di finanziamento adatto per gli ingenti investimenti necessari. Lo scopo della normativa in questione è quindi quello di attirare sempre più capitali privati nel settore europeo delle telecomunicazioni;

3.4) Delibera Agcom n. 9/2023.

La Delibera Agcom n. 9/2023 è stata emanata dall'Autorità per le garanzie nelle comunicazioni [122] con lo scopo di adottare le linee guida finalizzate all'attuazione dell'art. 7-bis del D. L. 30 aprile 2020, n. 28 [123] in materia di "*sistemi di protezione dei minori ai rischi del cyberspazio*".

La Delibera in questione è finalizzata anche nel definire quali siano le linee guida e i requisiti minimi ai quali un internet service provider deve ottemperare per poter considerare il suo operato a norma.

Il D. L. n. 28/2020 ha imposto l'istallazione, da parte degli operatori ISP, di sistemi di Parental Control, visti come dei filtri per contenuti inappropriati ad un pubblico di minori di anni diciotto, che devono rispettare le seguenti condizioni:

- Devono essere pre-attivati di default in caso di contatto con i minori: "*a riguardo gli operatori rilevano che la pre-attivazione dei sistemi di parental control non dovrebbe riguardare le linee sottoscrivibili solo da consumatori maggiorenni, […] pertanto propongono un sistema pre-attivato solo nel caso di offerte riservate ad un pubblico di minorenni [124]*"
- Devono essere totalmente gratuiti;
- Devono essere disattivati solo su richiesta dei consumatori;
- Devono essere necessariamente accompagnati da informazioni trasparenti, adeguate e aggiornate in merito alla disponibilità e al corretto utilizzo del servizio fornito.

Ciò che si cerca di correggere e di rafforzare tramite questa politica è il sistema dell'Age Verification, ossia: "*una tecnologia che si occupa di stabilire l'età dell'utente del servizio*

[122] L'Agcom fa parte delle autorità indipendenti e nasce con la L. 249 del 1997 con lo scopo di conciliare i rapporti tra gestore di servizi e l'utente finale. Le autorità indipendenti sono delle autorità amministrative nate intorno agli anni 90' che hanno le seguenti caratteristiche:

- Assenza di copertura costituzionale;
- Assenza di un indirizzo politico;
- Carattere indipendente.

Le Autorità indipendenti nascono con la L. n.481 del 1995 e si occupano di andare a regolamentare quei servizi considerati come essenziali, i quali erano precedentemente nelle mani del Monopolio dello Stato. L'indipendenza di queste Autorità dallo Stato è dovuta dal fatto che quest'ultimo ricoprirebbe un ruolo di concorrente e arbitro nella concorrenza e nel mercato.

[123] Art. 7-bis D.L. 30 aprile 2020 n. 28: "*sistemi di protezione dei minori dai rischi del cyberspazio*";

[124] Punto III, Delibera 9/2023: "*pre-attivazione dei sistemi di parental control*";

online al fine di impedire che un minore possa accedere ad un servizio a lui non rivolto o a lui potenzialmente pericoloso [125]". Tale sistema si è rivelato il più delle volte inefficace e facilmente eludibile.

In base a quanto esposto dall'art. 8 del GDPR [126]: "*un minore può concedere validamente il consenso al trattamento dei propri dati personali solo se ha raggiunto almeno i 16 anni di età […] in alternativa il consenso può essere legittimato con l'autorizzazione della responsabilità genitoriale*". Lo stesso articolo statuisce che gli stati membri possono per legge fissare un'età inferiore; in Italia, infatti, l'art. 2-quiquies del D.lgs. 101/2018 [127] consente l'espressione legittima del consenso al trattamento dei dati personali a partire dai quattordici anni.

Tuttavia, nonostante vi siano questi obblighi imposti dalla legge, le statistiche ci dicono che l'88% dei minori di età compresa tra gli undici e i tredici anni utilizza regolarmente i social network [128].

Questi dati fanno emergere come in realtà il sistema dell'Age Verification sinora utilizzato è risultato essere quasi del tutto inefficace e che c'è bisogno di una tecnologia più accurata e che garantisca un maggior grado di sicurezza, per questo è stata rivolta l'attenzione ai filtri DNS e ai sistemi di Parental Control.

In seguito ad un'attenta consultazione pubblica della delibera in questione, l'Agcom ha emesso una serie di linee guida sull'utilizzo del filtro DNS, un sistema che permette di filtrare i contenuti internet, basandosi sulla tecnologia conosciuta come: "*Domain Name System*[129]". Il filtraggio DNS permette quindi di bloccare specifici contenuti internet e di contrastare una quantità pari al 35% degli attacchi informatici che vengono commessi ogni giorno, intervenendo direttamente sulla ricerca effettuata dall'utente [130].

---

[125] B. Saetta; "Age verification e protezione dei dati personali", 2023, GDPR;

[126] Art. 8, Reg. (UE) 2016/679: "*condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione";*

[127] Art. 2-quinquies, D.lgs. 101/2018: "*disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016";*

[128] Università di Cassino e del Lazio Meridionale, Dipartimento di scienze umane, sociali e della salute, 2022, www.unicas.it;

[129] Il DNS è un sistema utilizzato per la risoluzione di nomi dei nodi della rete e degli indirizzi IP e viceversa. In pratica il DNS va a tradurre i nomi di dominio degli utenti indirizzi IP, in modo che i browser possano poi caricare le risorse internet.

[130] www.dnsfilter.com;

Le linee guida emanate dall'Agcom sull'utilizzo del filtro DNS vanno ad evidenziare quali sono le categorie di contenuti che necessitano di essere bloccate tramite un set di policy preimpostate, ossia:

- Contenuti per adulti, ad es. contenuti pornografici;
- Gioco d'azzardo e scommesse;
- Armi e uso di violenza;
- Siti che promuovono pratiche che possono danneggiare la salute;
- Anonymizer, intesi come "*proxy autonomi*[131]".

In base a quanto espresso dal punto II della delibera in questione [132], le linee guida e le regole definite dall'Agcom si applicano esclusivamente ai consumatori, escludendo la clientela affari. Le linee guida fanno genericamente riferimento agli utenti finali, i quali includono anche i clienti del settore business.

La questione maggiormente discussa con riferimento alle linee guida appena citate riguarda le possibili conseguenze in caso di non adeguamento a tali disposizioni.
In base a quanto sostenuto dall'Avv. e Data Protection Officer Vincenzo Gallotto si desume che [133]: "*non sono previste attività sanzionatorie da parte dell'Agcom in caso di mancata attivazione del Parental Control, ma sussiste comunque l'obbligo, in capo all'Autorità, di notificare e di segnalare l'anomalia all'operatore, così da garantire a quest'ultimo la possibilità di adeguarvisi entro un periodo di sessanta giorni*".
In caso di inottemperanza è prevista la possibile apertura di un procedimento.
Attraverso la Delibera in questione, in aggiunta alle linee guida, viene stilato anche un elenco di obblighi a cui gli operatori ISP devono ottemperare, i seguenti:

- integrare almeno un sistema di parental control basato su un filtro DNS o su altro filtro di rete, oppure che può essere scaricato tramite app da parte del consumatore;
- fornire un'interfaccia semplice e intuitiva, con informazioni che siano abbastanza chiare per l'attivazione, disattivazione e configurazione dell'utente;

[131] I server proxy sono dei sistemi che consentono all'utente che li utilizza di agire tramite anonimato, tagliando la connessione diretta tra client e server.
[132] Considerando II, Delibera 9/2023: "*ambito di applicazione*";
[133] V. Gallotto; "Parental Control, gli obblighi per i provider internet", 2023, www.studiolegalegallotto.it;

- Includere nel prezzo del servizio offerto la funzionalità minima di sblocco dei contenuti vietati ai minori;
- Adeguarsi alle disposizioni e comunicare il partner entro 9 mesi dalla pubblicazione della delibera;
- Rimborsare, entro un limite di tempo di sessanta giorni, le somme addebitate agli utenti in caso di protezione non idonea e di violazione degli obblighi.
- scegliere fra le soluzioni di protezione internet offerte dal mercato, senza vincoli tecnologici o di dimensione, purché sia garantito il controllo minimo dei contenuti vietati per legge;
- aggiungere eventualmente servizi a pagamento, nella massima trasparenza dei costi, come ad es: sblocco per un tempo configurabile, previa autorizzazione del titolare del contratto, programmazione per fasce orarie e memorizzazione dei siti visitati; personalizzazione dei contenuti aggiuntivi rispetto a quelli minimi.

La Delibera in esame presenta però alcune criticità non di poco conto [134]:

- La prima riguarda la delicatezza e la complessità che caratterizzano la regolamentazione di questo settore.
  Spesso, infatti l'approvazione di delibere come quella in questione, richiede un'attenta e profonda cognizione del mondo giuridico, ma tale conoscenza del diritto, il più delle volte, non si estende a settori di tipo tecnico-informatici come quello in questione, spesso quindi non si è in grado di comprendere la complessità dell'argomento che si sta trattando e questo porta alla commissione di determinati errori o equivoci;
- La seconda invece è rappresentata dal fatto che tale sistema di filtraggio DNS presenta in realtà non pochi svantaggi, come ad es:
  a) Le risposte DNS possono essere falsificate con lo scopo di reindirizzare l'utente verso siti illegittimi e dannosi;
  b) I vari hacker e criminali che operano in rete, per eludere la loro tracciabilità, registrano costantemente nuovi nomi di dominio, spostandosi in diverse zone del web e rimanendo inosservati;

[134] TitanHQ; ""DNS filtering: the how-to guide", 2021, www.titanhq.com;

c) I filtri DNS possono essere facilmente aggirati o elusi attraverso l'utilizzazione di server proxy che gli permettono di nascondere il loro IP originale e ottenere l'accesso all'indirizzo IP richiesto dal DNS;
d) La procedura di modifica del protocollo DNS presenta un'elevata complessità che potrebbe addirittura generare problemi di sicurezza o malfunzionamenti tecnici imprevisti.

Analizzando, quindi, la Delibera 9/2023 e le proposte da essa avanzate, possiamo concludere che l'adozione di un sistema di Parental Control che sia dotato di una tecnologia di filtraggio DNS potrebbe sicuramente garantire alcuni benefici in termini di sicurezza per gli utenti (minori e non minori), ma allo stesso tempo si potrebbe rivelare come qualcosa di inefficace e non necessario a causa delle problematiche precedentemente analizzate.

CONCLUSIONI

Alla luce di quanto evidenziato nell'elaborato, appare abbastanza chiaro che la tematica della responsabilità dell'ISP ha subito, nel corso del tempo, una significativa evoluzione e modifica nei contenuti e nel perimetro, pur preservando le criticità e le necessità di fondo, ponendo il tema all'attenzione di giudici e legislatori internazionali, soprattutto in relazione al rapporto con il mondo digitale e dei social network.
La questione chiave, trattata dall'elaborato, si basa sul verificare se, e in caso come, la responsabilità del provider possa essergli imputata, in relazione agli illeciti commessi sulle piattaforme digitali di loro competenza.
Ciò che, spesso, è alla base dell'imputazione di una responsabilità del genere è la necessità di individuare un responsabile per le violazioni commesse, e spesso, il colpevole più facilmente rintracciabile rimane il provider stesso.
Allo stesso tempo è però evidente che non si possa addossare al provider un regime di responsabilità troppo rigido, poiché in tal caso il regime in questione andrebbe a provocarne l'inibizione o addirittura a ridurne l'attività; ciò porterebbe a conseguenze negative facilmente prevedibili sullo sviluppo dell'internet e delle sue enormi potenzialità.

Come affrontato nell'elaborato, negli ultimi anni ci sono stati numerosi interventi normativi che hanno apportato modifiche e cambiamenti sia sul mondo del digitale che sull'inquadramento del ruolo e della responsabilità del provider (quali ad es. il DMA e il DSA), ma ciò che permane è una necessità sempre maggiore di disciplinare il corretto utilizzo delle tecnologie internet e delle funzioni di condivisione di contenuti, specialmente se si fa riferimento ai social media.

Nei capitoli precedenti sono state messe in risalto le caratteristiche principali dei contenuti che vengono pubblicati online quotidianamente: la dinamicità e l'enorme quantità, le quali rappresentano l'ostacolo maggiore ad una disciplina univoca della materia.

Per via di queste due caratteristiche appena menzionate, rimane sempre molto complicato, se non impossibile, eseguire un controllo su ogni contenuto o informazione che vengono diffusi sulle piattaforme digitali ogni giorno; per di più i meccanismi di difesa per la repressione degli illeciti non si sono rivelati così efficaci e la figura dell'ISP non sembra aver ricevuto ancora una disciplina del tutto univoca e completa. Tutto questo porta ad un incremento esponenziale della commissione degli illeciti online.

Pertanto, ciò che si rende necessario è, in primo luogo, una dettagliata disciplina relativa alla notificazione e alla rimozione del contenuto illecito, in secondo luogo, un accurato sistema di controllo e di sanzioni a tutela dell'intero sistema.

Il tutto dovrà naturalmente essere costituzionalmente orientato, in quanto il provider, nello svolgimento delle sue funzioni di controllo e gestione, dovrà necessariamente rispettare i diritti fondamentali degli utenti.

Infine, relativamente alla possibilità di individuare gli utenti che hanno commesso l'illecito, occorrerebbe implementare un meccanismo più efficace e sofisticato di individuazione degli utenti online.

Come ovvio, internet rappresenta uno degli strumenti più facili attraverso i quali si possono compiere dei reati e delle azioni in via anonima e la possibilità di identificazione della persona sussiste di regola solo se il soggetto decide di mostrarsi per ciò che realmente è.

A ciò deve seguirsi il fatto che, in Italia come all'Estero, sia pur secondo diverse declinazioni ed interpretazioni, sul provider non incombe alcun obbligo di accertamento della reale identità del soggetto che ha ipoteticamente realizzato la violazione.

Detto ciò, abbiamo compreso quanto sia complessa e intrecciata la materia trattata dall'elaborato in questione, ma anche quanto importante sarebbe una disciplina unitaria e conforme a riguardo.
Il dibattito è tuttora molto accesso, così come numerose sono le decisioni che si sono interessate e proseguono ad affrontare la materia della responsabilità degli ISP; occorre quindi tenersi aggiornati sui successivi sviluppi normativi e giurisprudenziali.

Bibliografia

A. Ingrassia: "il ruolo dell'ISP nel cyberspazio: cittadino, controllore o tutore dell'ordine?", 2010, par. 1.2, pagg. 5 e 6;

Ansa, "USA, due terzi delle persone leggono notizie sui social", su Ansa.it, 2017;

A.P. Komminos, The Digital Markets Act How does it compare with competition law, ius.giuffrefl.it, 2022;

Art. 1 par. 1 Dir. n. 31/2000;

Art. 1 co.1 D.lgs. 70/2003;

Art. 1 par. 1 lett. b) Dir. 2015/1535;

Art. 2 Dir. n. 98/34/CE;

Art. 2 lett. B, Dir. n. 31/2000;

Art. 2 lett. F, Dir. n. 31/2000;

Art. 2-quinquies, D.lgs. 101/2018: "*disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016";*

Art 3 co.1 Reg. 2120/2015;

Art 4. Par. 25 GDPR;

Art. 5 Dir. n. 31/2000;

Art. 6 Dir. 31/2000;

Art. 6 D.lgs. 70/2003;

Art. 7-bis D.L. 30 aprile 2020 n. 28: "*sistemi di protezione dei minori dai rischi del cyberspazio;*

Art. 7 Reg. n. 2120/2015;
Art. 8 Reg. n. 2120/2015;
Art. 8, Reg. (UE) 2016/679: "*condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione";*
Art. 9 Reg. n. 2022/1925;
Art. 10 co.1 Lett. b) Dir. n. 97/33/CE del Parlamento Europeo e del Consiglio sull'interconnessione nel settore delle telecomunicazioni e finalizzato a garantire il servizio universale e l'interoperatività attraverso l'applicazione dei principi di fornitura di una rete aperta (ONP);
Art 10 co. 1 Reg. n. 2022/1925;
Art. 11 Carta di Nizza;
Art. 14 par. 1 Dir. 31/2000/CE;
Art. 15 co.1 Dir. n. 31/2000;
Art. 17 co.1 Direttiva n. 790/2019 del Parlamento e del Consiglio Europeo;
Art. 17 co. 2;3 e 4 Dir. n. 790/2019 del Parlamento e del Consiglio Europeo;
Art.17 D.lgs. 70/2003,
Art. 17 Reg. n. 2022/1925;
Art. 102 TFUE, ex art. 82 TCE;
Art. 2086 c.c.;
Avv. A. Calia; "Diritto e tecnologie digitali, quali vantaggi e quali rischi?", Università degli studi di Cagliari, 2019, pag. 7;
Avv. F. Molinari, "nascita, evoluzione e funzionamento della rete", Diritto.it, 2008;
Avv. P. Severino: "controlli e controllori. Nuovi diritti e posizioni di garanzia nel cyberspazio", Libera Università degli studi sociali Guido Carli, 2022;
Boston Consulting Group, Sizing the digital economy, 2020;
B. Saetta; "Age verification e protezione dei dati personali", 2023, GDPR;
C-360/10 CGUE, Sez. III;
Cass. Civ. Sent. n. 7708/2019;
Cass. Civ. Sent. n. 10893/2011;
Cass. pen., Sez. III, 17 dicembre 2013 (dep. 3 febbraio 2014), n. 5107;
Causa C-401/2019 Corte Europea, Grande Sezione;
COM/2016/288/final;

Com. n. 97/157, Commissione europea;
Cfr. G. De Nova, F. Delfini, La direttiva sul commercio elettronico: prime considerazioni, in «Rivista di diritto privato», 2000, vol. 2, fascicolo 4, pp. 693-704;
D. Aliperto: Digital Services Act, Breton: "Non è ministero della Verità ma chance per le Big tech", Corcom, 2023;
D.lgs. 8 giugno 2001, n.231, disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11, L. 29 settembre 2000, n. 300;
D. L. n.70 del 2020;
D.L. n. 2023/123;
D. M. Boyd; N. B. Ellison, social network sites: definition, history, and scholarship; Journal of Computer-Mediated communication, Vol. 13, issue 1, 2007;210-230;
Dir. 22/2002/CE;
Dir. n. 48 del 2004;
Dir. 97/7/CE;
Dir. 98/48/CE;
F. Meta, "Butti all'UE, rinviare la proposta in attesa di dati certi", Corcom, 2023;
F. Sorensen, 2022 Fair Share discussion and 2012 BEREC statement to ITU/WCIT, Nkom, 2022;
G. Muscolo, the Digital Market Act and the asymmetric regulation for platforms, Ius.giuffrefl.it, 2022;
G.M. Riccio; la responsabilità degli internet service provider, situazione legislativa e problemi aperti, in V. D'Antonio; S. Vigliar, studi di diritto della comunicazione, persone, società e tecnologie dell'informazione, Padova, Cedam, 2009;
G. Ponte; G. Robustelli, "si scrive Fair share, si legge Fair play", Tim, 2023;
I. Genna; Fair Share, come Bruxelles potrebbe riscrivere le regole di internet, 2023, par. 1;
J. Hoffman; 29 Internet experts and academics send a letter to the Commission urging to abandon the sending party network pays proposal, 2022, komatis.org;
K. Schwab; S. Zahidi, The future of Jobs Report 2020, World Economic Forum, 2020;
M. De Cata, la responsabilità civile dell'internet service provider, Milano, Giuffrè Editore, 2010;

M.Iaselli, “Internet Service Provider, guida all’ISP: cos’è, tipologie e regimi di responsabilità”, Wolters Kluwer, Altalex, 2019;
N. Newman; R. Fletcher; A. Schulz; S. Andi; C.T. Robertson; R.K. Nielsen, “Digital news report 2021”, Reuters Institute for the study of journalism, X Ed., Università di Oxford, 2021;
P. Licata: “Tlc, Breton: Fair Share non basta, presto un Digital networks act”, Corcom, 2023;
Punto III, Delibera 9/2023: “*pre-attivazione dei sistemi di parental control*”;
P. Sanna, Il regime di responsabilità dei providers intermediari di servizi della società dell’informazione, Milano, Giuffrè Editore, 2004, pp. 279-302;
R. Ristuccia; L. Tuffarelli, la natura giuridica di internet e le responsabilità del provider, Interlex, 1997, par. 2.1.;
Reg. (UE) n. 531/2012 del Parlamento Europeo e del Consiglio del 13 giugno 2012, relativo al roaming sulle reti pubbliche di comunicazioni mobili all’interno dell’Unione, punto 2;
Reg. (UE) n. 531/2012 del Parlamento Europeo e del Consiglio del 13 giugno 2012, relativo al roaming sulle reti pubbliche di comunicazioni mobili all’interno dell’Unione, punto 3;
S. Saracco: “il fenomeno dell’E-commerce e i recenti sviluppi del mercato unico digitale in Europa”, Giureta 2016, vol. XIV, pag. 94;
T.Gillespie: “the politics of platforms”, 2010, Vol. 12, pp 347-364;
TitanHQ; “DNS filtering: the how-to guide”, 2021, www.titanhq.com;
Treccani, enciclopedia online, https://www.treccani.it/enciclopedia/social-network/;
United Nations, Sustainable Development Goals 16, 2015;
Università di Cassino e del Lazio Meridionale, Dipartimento di scienze umane, sociali e della salute, 2022, www.unicas.it;
V. Gallotto; “Parental Control, gli obblighi per i provider internet”, 2023, www.studiolegalegallotto.it;
V. Giannotti, Fondamenti di informatica, Università degli studi di Verona, 2016, cap. 2;
www.dnsfilter.com ;