



UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII

Dipartimento di Ingegneria
dell'Informazione



unIMC

Antitrust e protezione dei dati personali. Quale rapporto?

Anna Licastro, PhD student

Dipartimento di Scienze Giuridiche e Sociali.

Università degli Studi «Gabriele D'Annunzio» di Chieti-Pescara

anna.licastro@unich.it

Martedì 19 Luglio 2022



Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data
Protection

Perché l'antitrust si sta interessando della protezione dei dati personali?

(La sicurezza dei dati e la protezione dei dati personali non sono obiettivi diretti della politica di concorrenza).



Antitrust: la tutela della concorrenza.



- Cosa significa tutelare la concorrenza?
 1. Proteggere il buon funzionamento dei mercati;
 2. assicurare ai consumatori il massimo benessere perseguibile.

- Le norme a tutela della concorrenza vietano: le condotte delle imprese che hanno raggiunto un potere di mercato così elevato da essere in grado di allentare la pressione competitiva e, di conseguenza, ostacolare la rivalità (fisiologica) con imprese concorrenti.

- Le condotte vietate sono: **abusi di posizione dominante**, concentrazioni, intese e cartelli.

- L'**abuso di posizione dominante**: lo sfruttamento illecito della potenza economica raggiunta da un'impresa sul mercato che le consente di avere comportamenti alquanto indipendenti nei confronti dei suoi concorrenti, dei clienti e dei consumatori. La posizione di dominanza le permette di mettere in atto le proprie strategie commerciali senza subire condizionamenti particolari da parte degli altri attori del mercato di riferimento.

GDPR: protezione dei dati personali.



- Con il Reg.UE 679/2016, l'Unione Europea ha inteso garantire il diritto fondamentale sancito dall'art. 8, par.1 Carta dei diritti fondamentali dell'Unione Europea: «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano». In tal senso, anche l'art. 16, par.1 TFUE.
- Il diritto all' «autodeterminazione informativa»: il diritto della persona di decidere da sé circa la cessione e l'uso dei propri dati personali. (Corte Costituzionale federale tedesca, sentenza 15.12.1983).
- «Il consenso non dovrebbe essere considerato come dato liberamente se la persona interessata non dispone di un'effettiva libertà di scelta o non è in grado di negare o revocare il consenso senza pregiudizio» (CNIL, *Facebook Ireland Limited*, délibération n. 24, 31 dicembre 2021).
- **E se l'interessato si trovasse, di fatto, «costretto» a cedere i suoi dati per poter accedere ad un servizio? Sarebbe un'ipotesi di «consenso non dato liberamente» per cui il trattamento dei dati sarebbe illecito. Giusto?**

La prima contaminazione fra antitrust e protezione dei dati personali: **Bundeskartellamt v. Facebook (2019)**.



- L'autorità garante della concorrenza tedesca (*Bkart*) apre un'istruttoria a carico di Facebook per abuso di posizione dominante. Se l'utente vuole usare il *social network* deve prestare il proprio consenso ai termini di servizio al fine di concludere il contratto. I termini prevedono che Facebook raccolga i dati personali dei propri utenti, anche al di fuori della piattaforma, mediante i *Facebook business tools* di cui si avvalevano siti web di proprietà di terzi, come specificato nell'informativa.
- La modalità di acquisizione del consenso «*take it or leave it*» non lascia l'utente libero di scegliere fra opzioni differenti. È «obbligato» a prestare il consenso, pena la rinuncia all'iscrizione sul *social network*.
- Violazione della Legge sulla concorrenza tedesca per abuso di posizione dominante (imposizione di condizioni contrattuali inique) nonché violazione del GDPR in quanto l'utilizzo e la combinazione dei dati personali è avvenuta senza il valido consenso dell'utente e, dunque, il trattamento non è lecito ex artt.6 e 7, par.4, GDPR.
- Il fulcro della decisione: **la violazione non consiste tanto nell'uso dei dati da parte di Facebook, quanto nell'uso dei dati senza il valido consenso degli utenti.**

L'importanza del fattore umano.



(Tesi Bkart): solo Facebook è in grado di porre in essere una strategia commerciale tale da costringere gli utenti a prestare il consenso in modo non valido comprimendone, di fatto, la libertà di scelta. Se gli utenti avessero la possibilità di rivolgersi ad un *social media* alternativo non accetterebbero di iscriversi messi di fronte all'evidenza che i dati in Facebook ed off-Facebook sono trattati senza il loro valido consenso.

Attenzione! La decisione viene impugnata dinanzi al Tribunale regionale superiore di Düsseldorf il quale, nell'accogliere il ricorso presentato da Facebook, si è così pronunciato: « (...) **il mancato apprezzamento da parte degli utenti delle condizioni di contratto non era legato alla posizione dominante di Facebook nel mercato quanto all'indifferenza tipica dell'utente medio della piattaforma**».

Tra l'altro, la decisione è stata nuovamente impugnata innanzi alla Corte Federale di Giustizia tedesca nel 2020, la quale ha ritenuto che l'elisione delle possibilità di scelta avrebbe pregiudicato l'autonomia decisionale degli utenti e, dunque, il diritto all'autodeterminazione informativa.

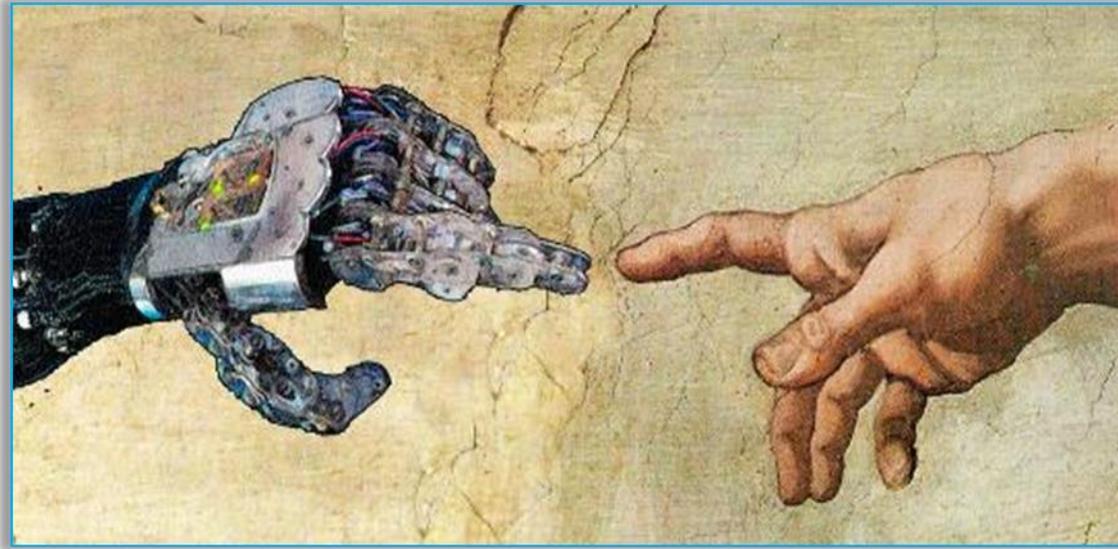
Nel 2021, il Tribunale di Düsseldorf ha rimesso la questione alla Corte di Giustizia dell'Unione Europea.

E se fosse, allora, un problema di *privacy paradox*?



- Contrariamente a quanto dedotto dal *Bkart*, il Tribunale di Düsseldorf ha ritenuto che, non era affatto certo che se gli utenti avessero avuto la possibilità di graduare il livello di informazioni condivise con la piattaforma, avrebbero scelto una soluzione *privacy-preserving*.
- Per *privacy paradox* (Norberg *et al.*, 2007) intendiamo il fenomeno in base al quale gli utenti percepiscono come impellente il bisogno di tutelare i propri dati personali, ma poi all'atto pratico decidono di fruire di un determinato servizio, nonostante siano ben consapevoli del livello minimo di protezione cui i propri dati verrebbero esposti.
- È evidente la discrepanza fra quello che il consumatore considera razionalmente giusto e le scelte di consumo che poi compie in concreto.

Una soluzione per risolvere il *privacy paradox*.



- Intervenire sull'*interface design*: obbligare i *designers* coinvolti dalle *big tech companies* nella progettazione delle interfacce grafiche a non manipolare le scelte dell'utente, facendo leva sui suoi *bias* cognitivi. Ad esempio, inducendolo a conferire più dati del dovuto o rendendogli più complicato rifiutare determinate opzioni e più semplice accettarle.
- La regolazione potrebbe arginare il potere economico dei giganti del web, ma sono, *in primis*, gli utenti a dover comprendere che i dati sono *assets* strategici per il mercato. Dovrebbero perciò avere maggiore consapevolezza circa le modalità con cui le grandi società del digitale trattano i dati per conseguirne vantaggi competitivi illegali.

D'altro canto, Tim Berners-Lee, inventore del World Wide Web,
sostenne:
«Il Web è più un'innovazione sociale che un'innovazione
tecnica».

