CAMERA DEI DEPUTATI – COMMISSIONE IX
AUDIZIONE DEL SEGRETARIO GENERALE
DELL'AUTORITÀ GARANTE
DELLA CONCORRENZA E DEL MERCATO

AVVOCATO FILIPPO ARENA

in merito all'indagine conoscitiva "*Sulle nuove tecnologie nelle telecomunicazioni con particolare riguardo alla transizione verso il 5g e alla gestione dei big data*".

Roma, 18 settembre 2019

Onorevole Presidente, Onorevoli Deputati,

Vi ringrazio per aver offerto all'Autorità Garante della Concorrenza e del Mercato l'opportunità di contribuire all'indagine conoscitiva sulle nuove tecnologie nelle telecomunicazioni. Il tema della sicurezza cibernetica delle reti, che la Commissione ha chiesto di approfondire, presenta un indubbio connotato tecnico, ma si intreccia nondimeno con una pluralità di aspetti legati alla tutela della concorrenza e del consumatore nell'economia digitale.

Come è noto, il 5G costituisce il prossimo *standard* tecnologico per lo sviluppo delle reti mobili. Le reti mobili di quinta generazione saranno in grado di trasmettere dati con una velocità 14 volte maggiore rispetto alle reti 4G, consentendo di coprire capillarmente il territorio e di connettere un elevatissimo numero di dispositivi in modo affidabile e con bassa latenza. Tale tecnologia non comporta solo un miglioramento significativo della qualità delle reti mobili, ma costituisce l'infrastruttura portante per lo sviluppo delle "*smart city*" e della

mobilità connessa, dell'*Internet of Things*, rendendo possibile la realizzazione di ecosistemi che rivoluzioneranno una molteplicità di settori economici (industria, sanità, agricoltura, ecc.).

L'Autorità – da diversi anni particolarmente attenta allo sviluppo delle reti di telecomunicazione a banda ultra-larga – nell'ambito della propria attività di *advocacy*, ha sostenuto e auspicato la rapida ed efficace transizione al sistema 5G.

In particolare, nel marzo 2018, l'Autorità si è pronunciata[1] in relazione alle regole per la messa a gara dello spettro necessario per lo sviluppo della tecnologia 5G, anche al fine di assicurare che il processo di assegnazione delle frequenze per i servizi di comunicazione mobile a banda larga costituisse un'opportunità per l'ingresso e l'affermazione di nuovi operatori, allo scopo di ridurre il livello di concentrazione nel mercato. Come è noto, l'asta per l'assegnazione delle frequenze 5G ha generato introiti di oltre 6 miliardi di euro e il nuovo entrante Iliad è riuscito ad acquisire blocchi di frequenze a 700 MHz, 3.700 MHz e 26 GHz.

L'Autorità ha più recentemente segnalato[2] gli ostacoli all'installazione di impianti di telecomunicazione mobile e *broadband wireless access* presenti nelle normative locali (comunali e provinciali) e regionali. Talune normative, infatti, fissano limiti e divieti ingiustificati o non proporzionati all'installazione di impianti di telecomunicazione o stabiliscono procedure amministrative di autorizzazione all'istallazione degli impianti difformi rispetto a quanto previsto

[1] AS1493 – PROCEDURE PER L'ASSEGNAZIONE DEI DIRITTI D'USO DI FREQUENZE PER FAVORIRE LA TRANSIZIONE VERSO LA TECNOLOGIA 5G, 14 marzo 2018.
[2] AS1551 – OSTACOLI NELL'INSTALLAZIONE DI IMPIANTI DI TELECOMUNICAZIONE MOBILE E BROADBAND WIRELESS ACCESS E ALLO SVILUPPO DELLE RETI DI TELECOMUNICAZIONE IN TECNOLOGIE 5G, 12 dicembre 2018.

dal quadro normativo statale. Inoltre, l'Autorità ha auspicato l'adozione di un indirizzo nazionale al fine di uniformare l'*iter* autorizzativo da seguire in caso di realizzazione di impianti di telecomunicazione, definendo chiaramente le procedure e i moduli da utilizzare e chiarendo le disposizioni che possono dar luogo a dubbi interpretativi e applicativi idonei a rallentare gli investimenti.

La rimozione degli ostacoli ingiustificati allo sviluppo delle reti 5G consente di promuovere la concorrenza nei mercati delle comunicazioni elettroniche con ricadute positive sui livelli di servizio erogati ai consumatori e alle imprese, nonché sulla competitività dell'Italia a livello internazionale. Si tratta di un aspetto di particolare rilevanza proprio nella fase attuale di investimento nelle tecnologie 5G, al fine di non vanificare l'impegno che l'Italia ha profuso muovendosi in anticipo rispetto ad altri Paesi europei nell'assegnazione delle frequenze.

*****

Un ulteriore aspetto di grande rilievo in relazione allo sviluppo delle reti 5G, attualmente al vaglio dell'Autorità, risiede negli accordi che gli operatori mobili stanno concludendo per la realizzazione congiunta e la condivisione delle reti 5G.

Nel mese di febbraio, Vodafone e TIM hanno annunciato di aver sottoscritto un Memorandum d'Intesa non vincolante in relazione a una potenziale *partnership* per condividere la rete attiva ed ampliare l'attuale accordo di condivisione dell'infrastruttura passiva. L'accordo si tradurrebbe in uno sviluppo congiunto dell'infrastruttura 5G, e riguarderebbe anche la condivisione degli apparati attivi anche delle rispettive reti 4G esistenti. Le due aziende, inoltre, stanno valutando

fattibilità e contenuti di una possibile aggregazione in una sola entità delle rispettive torri di trasmissione in Italia.

Anche Wind e Fastweb hanno recentemente annunciato un accordo strategico per lo sviluppo delle reti 5G, di durata decennale. La rete 5G condivisa dovrebbe includere sia macro siti che micro-celle, connessi attraverso la fibra di Fastweb, in grado di coprire il 90% della popolazione entro il 2026.

Tali accordi possono potenzialmente generare sinergie ed efficienze in termini di investimenti, ma possono anche avere significative ricadute concorrenziali. Si tratta, infatti, di accordi tra operatori concorrenti che hanno tradizionalmente sviluppato e gestito in autonomia le proprie reti mobili, potenzialmente idonei ad incidere sia sulla concorrenza statica che sulla concorrenza dinamica che caratterizza il settore. Al riguardo non è possibile allo stato aggiungere altro, posto che l'Autorità dovrà esaminare i diversi profili dei suddetti accordi.

Tematiche analoghe sono state, peraltro, esaminate dall'Autorità in occasione della valutazione dell'accordo di co-investimento tra TIM e Fastweb per la costruzione di una rete di telecomunicazioni fisse in fibra ottica (FTTH) destinata alla copertura di 29 tra le principali città italiane, mediante la società comune Flash Fiber Srl.

L'Autorità aveva infatti rilevato, in sede di avvio dell'istruttoria, come tale accordo fosse suscettibile di integrare un'intesa potenzialmente idonea a impedire, restringere o falsare in maniera consistente il gioco della concorrenza nei mercati della banda larga e ultra-larga. L'intesa, infatti, avrebbe potuto instaurare un rilevante grado di coordinamento tra le Parti su scelte strategiche relative alle reti fisse a banda larga e ultra-larga, riducendo l'intensità della

competizione statica e dinamica, considerato che tale cooperazione coinvolge i due principali operatori verticalmente integrati operanti nel settore.

L'Autorità ha poi concluso l'istruttoria rendendo vincolanti gli impegni presentati dalle parti, ritenendo quest'ultimi idonei a superare le iniziali preoccupazioni concorrenziali, valorizzando opportunamente le componenti di efficienza dell'accordo di co-investimento in essere tra TIM e Fastweb.

Si tratta di una decisione che mette ben in evidenza l'attenzione prestata dall'Autorità tanto alla concorrenza "statica" quanto alla concorrenza "dinamica" che si realizza attraverso investimenti e innovazione. Ciò nella consapevolezza dell'importanza strategica che le reti in fibra, come le reti 5G, avranno quali infrastrutture essenziali dell'economia e della società digitale.

*****

Gli accordi tra operatori concorrenti aventi ad oggetto lo sviluppo e la condivisione delle infrastrutture non costituiscono l'unico aspetto potenzialmente idoneo ad avere rilevanti ricadute concorrenziali. Tra le tematiche di ampio respiro connesse allo sviluppo delle reti 5G che possono avere un impatto significativo sulla concorrenza, particolare attenzione va prestata al principio della neutralità della rete (*net neutrality*).

La neutralità della rete è tutelata dall'art. 3 del Regolamento n. 2120/2015 (TSM – Telecoms Single Market – Regulation), rubricato "*Salvaguardia dell'accesso a un'Internet aperta*", che afferma il principio per cui tutto il traffico deve essere trattato in maniera uguale, senza discriminazioni, restrizioni o interferenze, e a prescindere dalla fonte e dalla destinazione, dai contenuti cui si è avuto accesso o

che sono stati diffusi, dalle applicazioni o dai servizi utilizzati o forniti, o dalle apparecchiature terminali utilizzate.

Nelle reti 5G le tecniche di *slicing* e di *orchestration* consentono di creare e gestire separazioni virtuali nelle reti, ottimizzando la connessione in funzione della tipologia del servizio. Ciò in quanto alcuni servizi potranno avere bisogno di una capacità di trasmissione elevata e continua mentre altri servizi avranno l'esigenza di connettere numerosi dispositivi che generano bassi livelli di traffico. L'architettura delle reti 5G, dunque, può consentire forme di *management* del traffico idonee a migliorare la *performance* e la flessibilità complessiva del sistema.

Ai sensi del vigente regolamento, il principio di neutralità non proibisce all'ISP (Internet Service Provider) di adottare misure ragionevoli di gestione del traffico. Tali misure sono considerate ragionevoli nella misura in cui sono non discriminatorie e proporzionate e non sono basate su considerazioni di ordine commerciale, ma su requisiti di qualità tecnica del servizio obiettivamente diversi di specifiche categorie di traffico; inoltre, tali misure non devono attribuire all'ISP la possibilità di controllare i contenuti specifici e sono mantenute per il tempo strettamente necessario.

In secondo luogo, in tre casi eccezionali, gli ISP possono adottare misure di gestione del traffico che vanno oltre il *management* ragionevole: *i*) quando vi è un obbligo legale in tal senso (si pensi ad esempio a disposizioni penali o di protezione del diritto d'autore); *ii*) per gestire una situazione di temporanea congestione della rete; nonché *iii*) per ragioni legate alla sicurezza della rete (ad es. per evitare attacchi cibernetici).

La neutralità della rete, dunque, non appare ad oggi costituire un ostacolo né agli investimenti né tanto meno alla sicurezza delle reti, ma rimane necessario per garantire un ecosistema Internet aperto e dinamico.

Il principio di non discriminazione, infatti, ha una forte valenza concorrenziale: gli ISP non possono vendere corsie preferenziali sulla banda larga ai produttori di contenuti digitali più ricchi e quindi maggiormente propensi a pagare per veicolare i propri contenuti più velocemente o con una migliore qualità. La neutralità della rete, dunque, garantisce parità di trattamento alle imprese attive nell'ampio ecosistema di Internet, stimolando l'innovazione. Si tratta di un obiettivo di *policy* particolarmente importante, anche alla luce dell'elevato livello di concentrazione che hanno raggiunto diversi mercati digitali e l'importanza di agevolare l'ingresso e la crescita sul mercato di *start-up* innovative.

Al contempo, il principio di neutralità della rete rappresenta uno strumento per garantire la libertà di espressione tanto degli utenti quanto dei fornitori di contenuti e servizi. Una libertà tutelata, tra l'altro, dall'art. 21 della Costituzione che stabilisce che tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione.

*****

Per quanto concerne il tema specifico della sicurezza delle reti in relazione agli apparati utilizzati per la loro realizzazione, si rileva come il 5G sia nato grazie a un processo di standardizzazione delle tecnologie nelle reti mobili guidato dal consorzio "*3rd Generation Partnership Project*" (3GPP), il quale unisce le organizzazioni internazionali di definizione degli *standard* nelle telecomunicazioni (ARIB – Giappone, ATIS – Stati Uniti d'America, CCSA -

Cina, ETSI - Europa, TSDSI - India, TTA - Korea, TTC - Giappone), e fornisce un ambiente condiviso per produrre le specifiche e i report che definiscono le tecnologie radiomobili. La prima versione dello standard 5G è stata approvata dal 3GPP nel 2018 e il suo sviluppo è in pieno regime. Nel 2020 è previsto il rilascio della seconda versione.

Le principali società che hanno fornito contributi tecnici allo *standard* sono Huawei (Cina), Ericsson (Unione Europea), Nokia (Unione Europea) e Qualcomm (Stati Uniti) e tali società sono anche tra i principali produttori dei dispositivi utilizzati nei vari livelli delle reti 5G, insieme ad altri *vendor* quali ZTE (Cina) e Samsung (Corea del Sud).

L'importanza strategica che avranno le reti 5G – non solo per le comunicazioni mobili, ma anche come infrastruttura di base per i nuovi ecosistemi digitali dell'IoT e delle *smart city*– impone la necessità di prestare una particolare attenzione alla sicurezza e all'integrità delle reti. In questo senso, le decisioni degli operatori in materia di sicurezza cibernetica possono potenzialmente generare esternalità sistemiche di grande impatto; nel lungo periodo, i costi per la società derivanti dai rischi di reti non sicure possono ben eccedere i risparmi conseguibili da un operatore nel breve periodo per l'acquisto di dispositivi meno costosi. Spetta, dunque, alle autorità competenti assicurare il rispetto di *standard* minimi di sicurezza tenuto conto dei rischi e dei costi complessivi che possono derivare dai rischi per l'integrità delle reti.
La sfida è quella di trovare l'assetto normativo e istituzionale più adeguato a conciliare il perseguimento di tale obiettivo con le esigenze di investimento imposte dalla continua innovazione tecnologica che caratterizza il settore delle reti di comunicazione elettronica.

Come è noto, il decreto Golden Power (Decreto legge 25 marzo 2019, n. 22, convertito, con modificazioni, dalla legge 20 maggio 2019, n. 41) individua i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G quali attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale. Viene altresì previsto che la stipula di contratti o accordi aventi ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti 5G, ovvero l'acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione, sono soggetti all'obbligo di notifica quando posti in essere con soggetti esterni all'Unione Europea.

Tali accordi rientrano, dunque, nella procedura di notifica di cui all'art. 1, comma 4, del D.L. 15 marzo 2012, n. 21, sebbene con possibili semplificazioni delle modalità di notifica, dei termini e delle procedure che possono essere definite con decreto del Presidente del Consiglio dei Ministri.

L'esigenza di un affinamento del quadro normativo riguardante i poteri speciali che interessano le reti con tecnologia 5G ha portato all'adozione del decreto legge 11 luglio 2019, n. 64, che integrava la disciplina in materia di esercizio dei poteri speciali, definiva una specifica regolamentazione procedurale, anche sotto il profilo delle tempistiche e dei rapporti con altre autorità amministrative, e introduceva altresì una disciplina procedurale specifica per l'esame delle notifiche inerenti ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G.

Per le note vicende politiche il decreto non è stato poi convertito; è ancora attuale, dunque, l'esigenza di sviluppo di una strategia e di un sistema normativo di ampio respiro in materia di sicurezza cibernetica. Ciò, peraltro, nell'ambito del quadro

europeo definito con il Regolamento 2019/881, che rafforza il ruolo dell'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione (ENISA) e introduce un sistema europeo per la certificazione della sicurezza informatica dei dispositivi connessi ad Internet e di altri prodotti e servizi digitali.

Non spetta all'Antitrust definire le soluzioni procedurali e tecniche più adeguate ad assicurare la tutela della sicurezza cibernetica. L'Autorità auspica, tuttavia, che le scelte legislative che saranno adottate a tal fine siano idonee a fornire alle imprese impegnate negli investimenti nelle nuove reti di comunicazione elettronica un quadro di riferimento trasparente e certo. Come l'Autorità ha avuto più volte modo di rilevare, infatti, l'incertezza delle regole è uno dei principali ostacoli alle scelte di investimento e impedisce il funzionamento di un mercato efficiente. Si tratta di costi particolarmente elevati proprio in quei settori ad alta intensità tecnologica e innovativa, nelle quali le imprese devono continuamente assumere decisioni di investimento.

In tale prospettiva, ad esempio, assumono importanza meccanismi *ex ante* – quali, ad esempio, quelli di certificazione – che possono consentire alle imprese di assumere consapevoli scelte di investimento e definire rapporti negoziali certi con i propri fornitori in uno scenario in cui lo sviluppo e la commercializzazione delle tecnologie avviene su scala globale.

L'esigenza di certezza può essere perseguita anche attraverso l'adozione di un testo organico e integrato in materia di sicurezza delle infrastrutture, che definisca un quadro di regole completo e trasparente, limitando il più possibile il ricorso a successivi decreti attuativi che ne possono rallentare l'attuazione.

Se le soluzioni tecniche per assicurare la sicurezza delle reti possono avere un costo non evitabile per imprese e cittadini, appare invece doveroso comprimere i costi derivanti da regole poco chiare, spesso di natura "emergenziale", la cui applicazione può generare un elevato grado di incertezza per gli operatori di settore.

*****

Il tema della sicurezza cibernetica, comunque, non interessa solo Parlamento e Governo, atteso che una strategia complessiva si compone di una varietà di strumenti di politica pubblica, che possono chiamare in causa anche l'Antitrust.

Ad esempio, tra le diverse misure previste dal Regolamento sulla cibersicurezza[3], l'Autorità intende evidenziare l'importanza degli sforzi volti ad accrescere la consapevolezza dei cittadini, delle organizzazioni e delle imprese circa le questioni riguardanti la sicurezza cibernetica. L'Autorità, infatti, ha da sempre evidenziato l'importanza che la fiducia dei consumatori riveste per lo sviluppo di un'economia digitale sana e competitiva. La promozione di tale fiducia, anche attraverso un processo di *empowerment* dei consumatori ha ispirato i numerosi interventi dell'Autorità volti alla repressione delle pratiche commerciali scorrette nel settore digitale.

Il Regolamento sulla cibersicurezza si muove nella stessa direzione laddove riconosce che le imprese e i singoli consumatori dovrebbero disporre di

[3] REGOLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

informazioni trasparenti in merito al livello di sicurezza (e al livello di affidabilità con cui è stata certificata la sicurezza dei loro) dei prodotti, dei servizi e dei servizi e dei processi delle tecnologie dell'informazione e della comunicazione.

Ciò è rilevante per consumatori e imprese sia in qualità di acquirenti che di utenti e costituisce anche un'occasione di riflessione per l'Autorità, al fine di comprendere se e in che misura i propri poteri in ambito di tutela dei consumatori potranno essere utilizzati anche con riguardo al tema della sicurezza cibernetica dei dispositivi e dei servizi offerti ai consumatori.

L'Autorità, ad esempio, è già intervenuta utilizzando i propri poteri in materia di tutela dei consumatori per affrontare la tematica dell'acquisizione dei dati personali da parte delle piattaforme *online*.

L'Autorità ha, in particolare, ritenuto che i modelli di *business* incentrati sulla raccolta ed elaborazione dei dati, anche quando l'utente riceve il servizio senza dover pagare un corrispettivo in termini monetari, rientrassero nella nozione di attività economica ai sensi del diritto europeo. A tal fine, l'Autorità, dando concreta attuazione a principi ormai consolidati sia a livello europeo che internazionale, ha ampliato la nozione di rapporto di consumo, riconoscendo la natura economica del comportamento dell'utente anche in relazione alle piattaforme digitali che offrono servizi gratuitamente.

Ciò posto, l'Autorità ha ritenuto ingannevole la schermata di registrazione ad un *social network* (Facebook) nella quale mancava un'adeguata e immediata informazione circa le finalità commerciali della raccolta dei dati dell'utente e ha ritenuto aggressive le modalità con cui il *social network* procedeva

all'acquisizione del consenso per lo scambio, per fini commerciali, di dati dei propri utenti con siti *web* o *app* di terzi[4].

In un altro caso, l'Autorità ha ritenuto aggressiva la condotta di un fornitore di un servizio di messaggistica (WhatsApp) consistente nell'aver di fatto forzato i propri utenti ad accettare nuovi Termini di Utilizzo – relativi all'utilizzo dei loro dati ai fini di profilazione commerciale e pubblicitari – facendo loro credere che sarebbe stato altrimenti impossibile proseguire nell'utilizzo dell'applicazione medesima[5].

L'effetto utile di tali interventi non è solo quello di fornire una tutela diretta ai consumatori, ma anche quello di svolgere un ruolo pro-concorrenziale nella misura in cui gli utenti sono posti nella condizione di esercitare (più) consapevolmente e attivamente le proprie scelte di consumo con riferimento al consumo di beni e servizi che raccolgono e utilizzano dati. Si tratta di un approccio che può essere rilevante tanto per trattare profili connessi alla *privacy* quanto per trattare aspetti connessi alla sicurezza informatica dei dispositivi e dei servizi offerti ai consumatori.

Il confine tra sicurezza e *privacy*, peraltro, è assolutamente labile dal momento che i due concetti si sovrappongono e sono intrinsecamente collegati: non vi può essere *privacy* senza sicurezza e l'assenza di sicurezza può indubbiamente comportare, tra gli altri, anche rischi concreti per la *privacy*.

*****

[4] Cfr. PS11112 - *Facebook-Condivisione dati con terzi*, 29 novembre 2018 n. 27432.
[5] Cfr. PS10601 - *Whatsapp-Trasferimento dati a Facebook*, 11 maggio 2017 n.26597.

Tali tematiche assumono ancor più rilievo nella prospettiva futura dello sviluppo del settore dell'*Internet of Things* e delle *Smart City* che le tecnologie 5G, come anticipato, alimenteranno. Si tratta di ecosistemi complessi, costituiti da un elevatissimo numero di dispositivi ed apparati connessi, in grado di dialogare tra loro e con il resto della rete, atteso che ogni dispositivo è connesso alla rete costantemente in modo tale da raccogliere, inviare e ricevere dati.

L'*Internet of Things* alimenterà, e per certi versi amplificherà, l'importanza dei Big Data per il funzionamento di una molteplicità di settori economici. I Big Data costituiscono un fenomeno ormai centrale nell'economia del XXI secolo, che l'Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni e il Garante per la protezione dei dati personali hanno analizzato nel corso di un'Indagine Conoscitiva per meglio comprenderne le implicazioni per la privacy, la regolazione, la tutela del consumatore e l'antitrust. Lo scorso mese di luglio sono state pubblicate le principali linee guida di cooperazione sul tema, nonché le raccomandazioni di *policy* condivise dalle tre Autorità. Il documento che raccoglierà i rapporti finali delle diverse Autorità sarà disponibile a breve.

I rischi per la sicurezza collegati all'IoT possono avere origine a diversi livelli: dai sensori utilizzati per raccogliere i dati, alle reti utilizzate per trasmettere quelle informazioni, alle piattaforme utilizzate per la fornitura dei servizi *data driven*. Tali rischi dipenderanno anche dalla fisionomia degli ecosistemi che si svilupperanno anche sotto il profilo economico e commerciale.

I dati raccolti a livello individuale possono essere elaborati al fine di offrire agli utenti un servizio migliore (ad esempio, in termini di *performance* e manutenzione del bene) o possono essere aggregati e utilizzati sia per migliorare il servizio in

questione (si pensi ai dati sulla mobilità urbana) che per generare ricavi attraverso la vendita di servizi diversi. Ad esempio, anche nel settore dell'IoT possono svilupparsi modelli di business tipici dei mercati a due (o più) versanti in cui i dati raccolti attraverso i dispositivi IoT sono valorizzati attraverso la vendita di servizi di pubblicità agli inserzionisti pubblicitari.

Sotto il profilo dell'utilizzo dei dati, inoltre, è possibile individuare diverse soluzioni e *business model* in considerazione dei diversi rapporti che possono instaurarsi tra il produttore del dispositivo e i fornitori dei servizi che utilizzano i dati generati dal dispositivo.

I dati generati da un dispositivo "*smart*" possono essere trasmessi – attraverso reti fisse o mobili – a un servizio di *cloud computing* dove possono essere analizzati anche al fine di fornire all'utente informazioni e/o servizi specifici. Il fornitore del servizio *cloud* può consentire all'utente anche l'accesso e il controllo remoto ai propri dispositivi. Si tratta di un modello che, sotto il profilo concorrenziale, solleva soprattutto potenziali criticità in tema di interoperabilità tra i dispositivi di produttori diversi. Ad esempio, sia il dispositivo che i servizi *cloud* connessi possono essere offerti da uno stesso operatore che utilizza protocolli proprietari, limitando o impedendo l'utilizzo di fornitori di servizio alternativi. Per converso, è possibile che i dati generati dal dispositivo *smart* siano resi disponibili anche a terze parti. La natura chiusa o aperta delle piattaforme e dei sistemi potrebbe avere riflessi, non solo sotto il profilo concorrenziale, anche sugli aspetti legati alla sicurezza cibernetica degli stessi.

Un diverso modello vede invece la comunicazione diretta tra dispositivi *smart* attraverso protocolli di comunicazione, senza l'impiego di un servizio intermedio. Sotto il profilo concorrenziale si tratta di un modello che potrebbe generare rischi

di *lock-in* legati alla compatibilità dei diversi dispositivi tra di loro. Anche sotto il profilo della sicurezza, si tratta di una soluzione che presenta caratteristiche diverse rispetto a quello precedentemente descritto.

Il fenomeno dell'IoT connesso allo sviluppo delle reti 5G per certi versi esaspera il ruolo dei dati nell'economia e nella società, dal momento che amplifica enormemente le fonti di dati – non solo le persone, ma anche le cose – e il loro utilizzo per offrire servizi e prodotti innovativi e sempre più personalizzati. La connessione degli oggetti alla rete determinerà un aumento esponenziale della quantità dei dati generati, della loro qualità e della loro ampiezza.

Tali cambiamenti saranno realizzati attraverso piattaforme ed ecosistemi nuovi, che potranno anche essere sviluppati e controllati da operatori con un significativo, e persistente, potere di mercato. Ciò può far sì che questioni concorrenziali possano intrecciarsi con questioni tecniche quali quelle relative alla sicurezza cibernetica.

Ad esempio, è stato rilevato che, in alcune circostanze, la promozione dei processi concorrenziali può richiedere l'accesso di imprese terze ai dati detenuti da un'impresa in posizione dominante.

Ciò può avvenire, ad esempio, attraverso forme di portabilità dei dati quali quelle attualmente prevista dal Regolamento sulla protezione dei dati personali ovvero tramite diversi livelli di interoperabilità. L'interoperabilità non costituisce solo un tema concorrenziale, ma può essere funzionale anche a perseguire obiettivi di sicurezza (e di *privacy*) laddove garantisca la compatibilità con un sistema di sicurezza selezionato dal fornitore e/o dall'utente. L'interoperabilità può realizzarsi tra prodotti concorrenti IoT, con sistemi di comunicazione e di

controllo per i suddetti prodotti o con servizi di *data analytics* che utilizzato i dati prodotti dai dispositivi.

In alcuni casi, si possono avere forme di interoperabilità a livello dei protocolli, ad esempio tra diversi servizi ovvero diversi dispositivi nell'ambito dell'IoT. In una prospettiva concorrenziale, tale interoperabilità consente lo sviluppo di servizi complementari che possono competere sul merito. Si tratta di una forma di interoperabilità che può richiedere lo sviluppo di *standard* ed è bene evidenziare come sia ormai opinione largamente condivisa che la segretezza dei protocolli non sia necessaria né spesso favorevole alla sicurezza, posto che quest'ultima è assicurata, piuttosto, dalla segretezza delle *password* e delle chiavi crittografiche.

In altri casi ancora, possono essere previste forme di interoperabilità dei dati, a livello di piattaforma o di rete di servizi complementari. Tale interoperabilità può consentire lo sviluppo di servizi complementari ad una piattaforma da parte di sviluppatori terzi consentendo agli utenti di scegliere ciascun servizio in maniera libera e indipendente. Una delle sfide dell'interoperabilità dei dati risiede nella sicurezza, ossia nell'assicurare che l'utente sia in grado di controllare l'utilizzo dei dati condivisi e il grado di sicurezza complessivo a tutela dei propri dati.

Infine, l'interoperabilità può essere piena laddove sia realizzata attraverso un'elevatissima integrazione e standardizzazione. Si tratta, ad esempio, del regime di interconnessione tra le reti di comunicazione elettronica.

Un diverso profilo di potenziale intersezione tra le questioni legate alla sicurezza cibernetica e la concorrenza risiede nello scambio di informazioni tra imprese concorrenti. Gli scambi di informazione tra imprese concorrenti possono violare

la normativa antitrust laddove determino, per oggetto o per effetto, una riduzione della concorrenza. Come hanno rilevato il *Department of Justice* e la *Federal Trade Commission* statunitense, tuttavia, è molto improbabile che una restrizione della concorrenza possa derivare da scambi di informazioni tecniche in materia di sicurezza cibernetica (ad esempio, su vulnerabilità e attacchi). Per contro, si tratta di scambi che di norma sono funzionali ad assicurare un elevato livello di sicurezza cibernetica dell'intero sistema.

Potrebbero, invece, rientrare pienamente nel divieto delle intese restrittive della concorrenza gli accordi o le pratiche concordate tra le imprese che abbiano come oggetto o effetto una riduzione dei livelli di sicurezza cibernetica di prodotti e servizi offerti a imprese e consumatori.

Ad esempio, alla fine del 2018, negli Stati Uniti, la società *leader* nei servizi di test sulla sicurezza cibernetica (NSS Labs Inc.) ha denunciato tre società che sviluppano *software* per la sicurezza cibernetica (CrowdStrike, Symantec ed ESET) per un'intesa volta a restringere la concorrenza attraverso la definizione e imposizione di uno *standard* per lo svolgimento dei test sui propri prodotti. La possibilità di svolgere test affidabili sui prodotti di sicurezza cibernetica appare particolarmente importante, atteso che il singolo utente difficilmente può verificare in modo diretto la *performance* tecnica di tali prodotti. Si tratta di un esempio, dunque, in cui la tutela della concorrenza può avere come portato immediato anche la tutela della sicurezza cibernetica.

Più in generale, è auspicabile che lo sviluppo delle reti 5G e dei nuovi ecosistemi dell'IoT avvenga assicurando non solo i più elevati livelli di sicurezza, ma anche i benefici di un pieno confronto concorrenziale. Ad esempio, se gli *standard* tecnologici appaiono di grande importanza per consentire investimenti efficienti

è altresì necessario che le procedure volte alla definizione di tali *standard* siano trasparenti, che le grandi multinazionali coinvolte rendano noti i brevetti essenziali in loro possesso e che le licenze siano rispettose dei termini FRAND, preservando la concorrenza tra le imprese che intendono utilizzare lo *standard* in questione. Anche eventuali *joint ventures* volte a sviluppare condizioni per l'interoperabilità di prodotti e servizi di operatori concorrenti dovrebbero adottare le necessarie cautele per far sì che tali attività non si traducano in restrizioni della concorrenza.

Tutelare la concorrenza in questo campo significa anche assicurare agli operatori che investiranno nei nuovi ecosistemi digitali un'effettiva possibilità di scelta tra offerte alternative e alimentare - anche potenzialmente oltre i necessari *standard* definiti a livello regolatorio - una competizione virtuosa tra i *vendor* sotto il profilo della sicurezza delle componenti tecnologiche che costituiranno tali ecosistemi.

INDAGINE CONOSCITIVA SUI *BIG DATA*

Analisi della propensione degli utenti *online* a consentire l'uso dei propri dati a fronte dell'erogazione di servizi

Primi risultati

I. Premessa

1. La presente indagine risponde all'obiettivo dell'Autorità di approfondire il rapporto – vieppiù cruciale per il funzionamento dei mercati - tra le imprese che forniscono i servizi digitali e gli utenti che forniscono dati personali nella prospettiva di questi ultimi. L'approfondimento è stato condotto attraverso una *survey* su un campione di utenti di servizi *online*, dei quali è stata indagata la propensione a consentire l'uso dei propri dati a fronte dell'erogazione di servizi. In particolare la *survey*, attraverso un ampio set di domande[1], ha affrontato tre questioni principali: i) il grado di consapevolezza degli utenti delle piattaforme digitali in relazione alla cessione e all'utilizzo dei propri dati individuali; ii) la disponibilità degli utenti a cedere i propri dati personali come forma di pagamento dei servizi *online*; iii) la portabilità dei dati da una piattaforma all'altra.

2. L'indagine si è svolta alla fine del mese di febbraio (dal 24 al 28 febbraio 2018) attraverso un questionario *online* rivolto a soggetti dai 16 anni in su che navigano in *internet* e accedono a piattaforme, applicazioni e servizi *online*. Hanno risposto 2.269 utenti. Nel campione le donne risultano leggermente più numerose (52,7%) rispetto agli uomini (47,3%). La fascia di età più rappresentata è quella tra 45 e 54 anni (24,3%) seguita dalla fascia 35-44 anni (18,3%) e da quella 45-54 anni (17,9%). Le aree geografiche più rappresentate sono Sud e Isole (39,6%) e Nord Ovest (26,2%). La maggioranza degli

[1] Il questionario si compone di 19 domande di cui alcune articolate in sotto-sezioni. Considerando tali articolazioni come singoli argomenti le domande salgono a 27.

intervistati ha un diploma di scuola media superiore (53,5%). La categoria professionale più rappresentata è quella degli impiegati e quadri (23,3%) seguita dai pensionati (17,2%)[2].

3. In estrema sintesi – per quanto riguarda il profilo della consapevolezza - i risultati dell'indagine mostrano che circa 6 utenti su 10 sono consapevoli del fatto che le loro azioni *online* generano dati che possono essere utilizzati per analizzare e prevedere i loro comportamenti e appaiono altresì informati dell'elevato grado di pervasività che il meccanismo di raccolta dei dati può raggiungere (ad esempio, sulla geo-localizzazione e sull'accesso di diverse *app* a funzionalità come la rubrica, il microfono e la videocamera) nonché delle possibilità di sfruttamento dei dati da parte delle imprese che li raccolgono.
Gli stessi risultati sembrano suggerire che esistono spazi di miglioramento per accrescere la consapevolezza degli utenti, infatti: i) la maggioranza degli utenti legge solo in parte le informative (54%) o non le legge affatto (33%); ii) gran parte degli utenti dedica un tempo limitato alla loro lettura; iii) un'ampia maggioranza del campione considera che le informazioni fornite possono risultare poco chiare.
Peraltro, anche utenti che non sono del tutto consapevoli della stretta relazione esistente tra cessione dei dati e gratuità del servizio, non di rado acconsentono all'acquisizione, utilizzazione e cessione dei propri dati personali. Gli utenti che invece negano il consenso lo fanno soprattutto in ragione dei timori di un improprio utilizzo dei propri dati: le preoccupazioni riguardano sia l'utilizzo a fini pubblicitari (46,7%) sia, ancor di più, l'utilizzo per altre finalità (50,2%).

4. Per quanto riguarda la disponibilità degli utenti a cedere i propri dati personali in cambio di servizi *online*, dall'indagine è emerso che 4 utenti su 10 sono consapevoli della stretta relazione esistente tra la concessione del consenso e la gratuità del servizio. Oltre i tre quarti degli utenti intervistati[3] dichiarano che sarebbero disposti a rinunciare ai

[2] In appendice si riportano le tabelle che illustrano la composizione del campione di rispondenti secondo sesso, età, area geografica, titolo di studio, professione e numerosità del nucleo famigliare.

[3] Da questo punto in avanti, per intervistati devono intendersi coloro che hanno fornito risposta alla domanda in esame.

servizi e alle *app* gratuite per evitare che i propri dati siano acquisiti, elaborati ed eventualmente ceduti. A fronte di ciò, comunque, solo la metà degli utenti dichiara che sarebbe disposta a pagare per servizi/*app* oggi forniti gratuitamente per evitare lo sfruttamento dei propri dati (pubblicitario o di altro tipo).

5. Infine, l'indagine ha evidenziato che attualmente solo 1 utente su 10 è consapevole dei propri diritti in materia di portabilità dei dati, anche se circa la metà degli utenti mostra interesse ad ottenere una copia dei propri dati. Lo scarso interesse all'utilizzo della portabilità è dovuto alla scarsa propensione ad utilizzare altre piattaforme/applicazioni (41,1%), ad una limitata sensibilità sulla rilevanza di tali dati (36,1%) nonché alla percezione di un'elevata complessità degli strumenti tecnologici (30,4%).

6. Di seguito verranno illustrate nel dettaglio le evidenze emerse dall'indagine presso gli utenti con riguardo a ciascuna delle questioni affrontate.

II. Il grado di consapevolezza degli utenti delle piattaforme digitali in relazione alla cessione e all'utilizzo dei propri dati individuali

7. La prima parte dell'indagine (domande 1-7) ha inteso approfondire quale sia l'approccio degli utenti delle piattaforme digitali al rilascio dei propri dati personali. Tale esperienza, infatti, pur coinvolgendo quotidianamente gli utenti in occasione della fruizione della maggio parte dei servizi *online* - dai social network, ai motori di ricerca, ai servizi di e-commerce –presenta dei risvolti e delle implicazioni che possono non risultare del tutto ovvi.

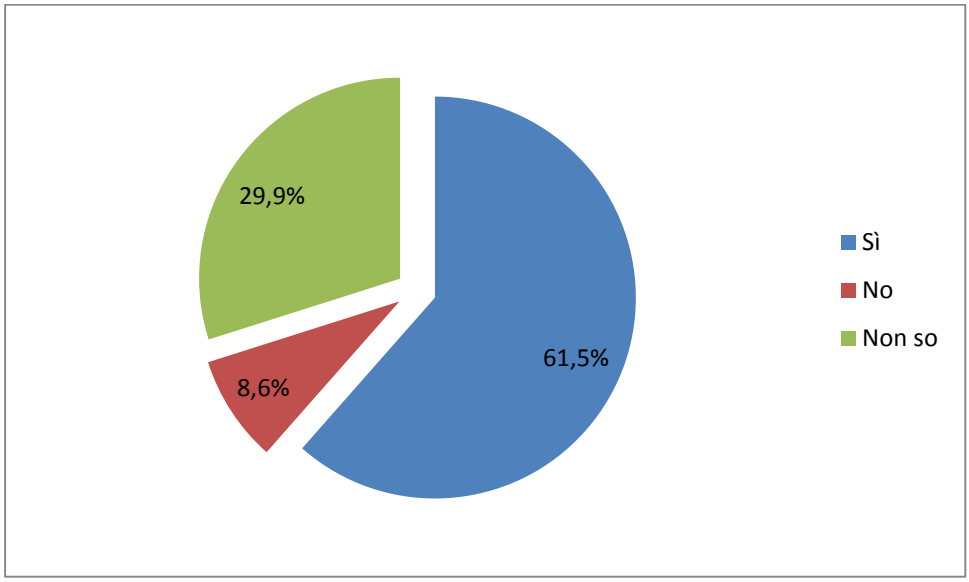
8. In questa prospettiva, tale sezione dell'indagine ha preliminarmente verificato quale sia il grado di consapevolezza degli utenti circa la portata dei dati che essi rilasciano (in termini di possibilità di analizzare e prevedere i loro comportamenti)[4], la

[4] Cfr. domande 1.1. e 1.2.

pervasività che tale meccanismo di raccolta a cui volontariamente si sottopongono può raggiungere[5] e l'importanza dei dati per le imprese che li raccolgono e utilizzano[6].

9. Le risposte del campione evidenziano che 6 utenti su 10 sono consapevoli del fatto che navigando in *internet* e utilizzando le applicazioni e i servizi *online* essi generano dati che vengono utilizzati per analizzare e prevedere i loro comportamenti (domanda 1.1, 61,5% degli intervistati) e che attivando i *cookies* essi acconsentono alla raccolta di tali dati da parte di soggetti diversi dai titolari dei siti e delle applicazioni (domanda 1.2, 60,6% degli intervistati) sugli aspetti sopra evidenziati.

Domanda 1.1 – "Per quanto a sua conoscenza
[navigando in internet e utilizzando app e servizi online i singoli utenti producono dati che consentono di analizzare i relativi comportamenti e di fare previsioni sui comportamenti futuri ai fini della comunicazione pubblicitaria e per altri scopi (ad esempio, campagne elettorali)?]"

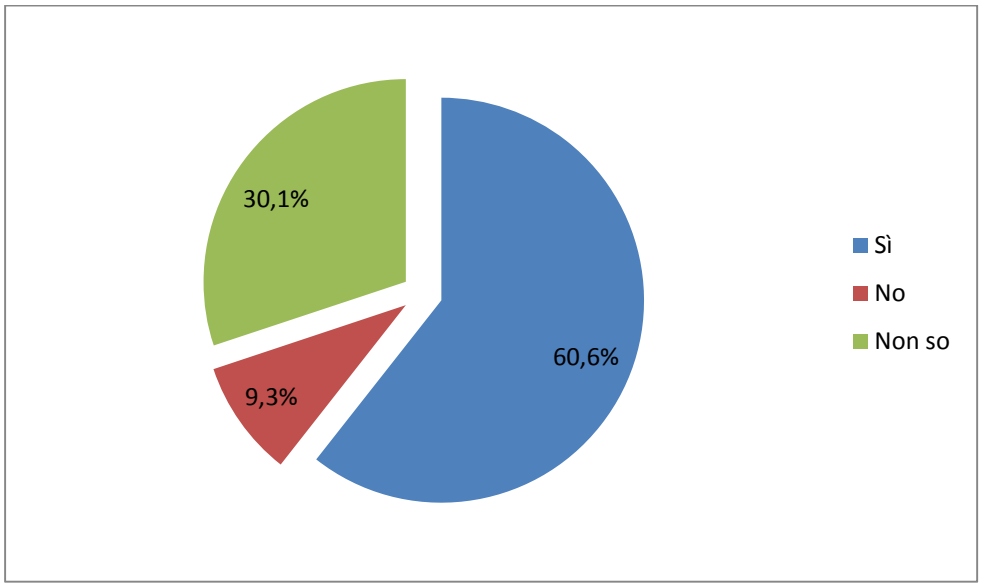


[5] Cfr. domande 1.3 e 1.4.

[6] Cfr domande 1.5 e 1.6.

Domanda 1.2 – "Per quanto a sua conoscenza

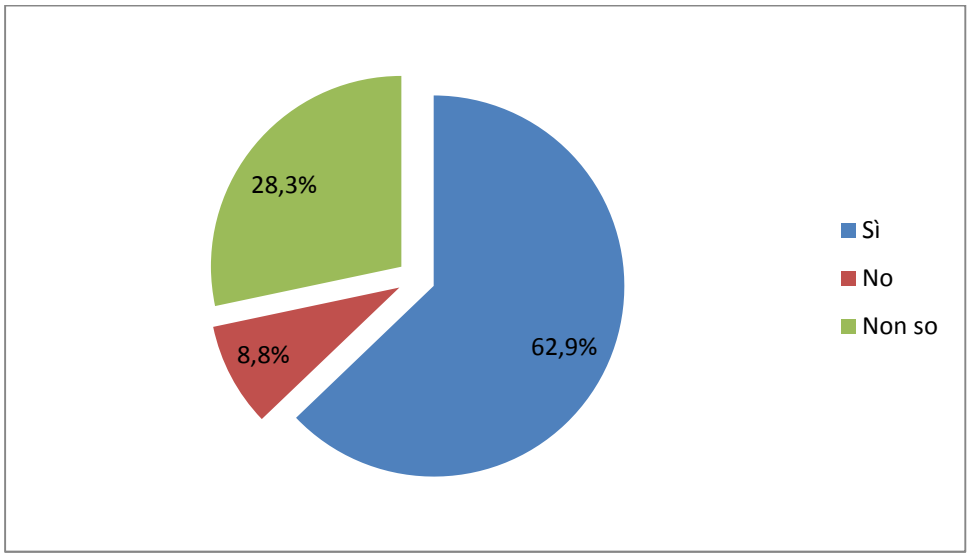
[navigando in internet e consentendo l'attivazione di cookies i singoli utenti consentono di raccogliere dati utili per analisi e previsioni sui relativi comportamenti ai fini della comunicazione pubblicitaria e per altri scopi (ad esempio, campagne elettorali)?]"



10. Di misura analoga è risultata la consapevolezza degli utilizzatori intervistati in merito al grado di pervasività che il meccanismo di raccolta dei dati *online* può raggiungere. In particolare, le risposte evidenziano che 6 utenti su 10 sono consapevoli del fatto che l'attivazione della funzione di geo-localizzazione sui *device* comporta la possibilità di individuare e tracciare con accuratezza la posizione e gli spostamenti degli utenti (domanda 1.3, 62,9% degli intervistati). Inoltre, circa la metà degli intervistati ha dichiarato di essere a conoscenza del fatto che diverse *app* hanno accesso a funzionalità importanti dei *device* come la rubrica, il microfono e la videocamera (domanda 1.4, 49,2% degli intervistati).

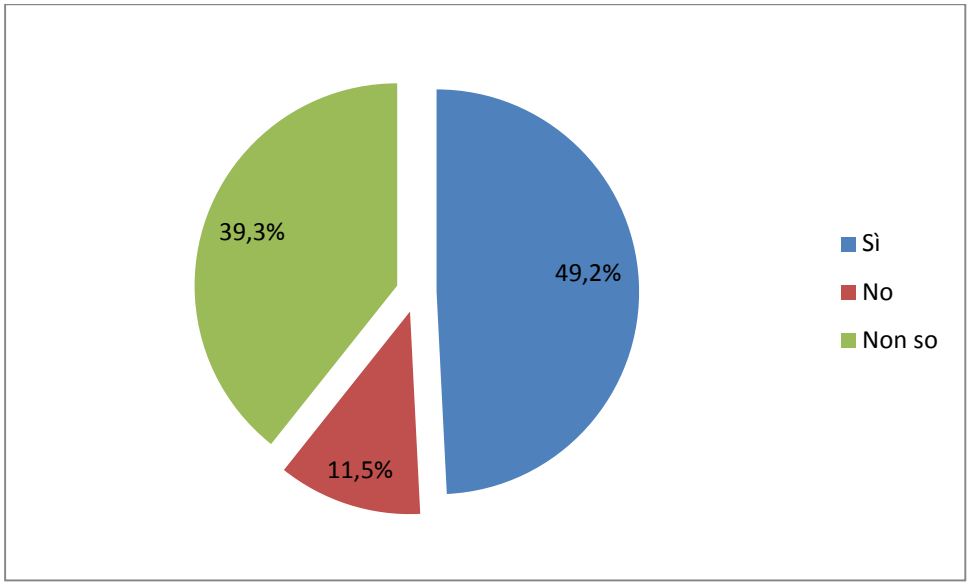
Domanda 1.3 – "Per quanto a sua conoscenza

[utilizzando smartphone e/o tablet con la funzione di geo-localizzazione attivata i singoli utenti producono dati che consentono ai fornitori di servizi internet di individuare la relativa localizzazione e tracciare gli spostamenti con accuratezza?]"



Domanda 1.4 – "Per quanto a sua conoscenza

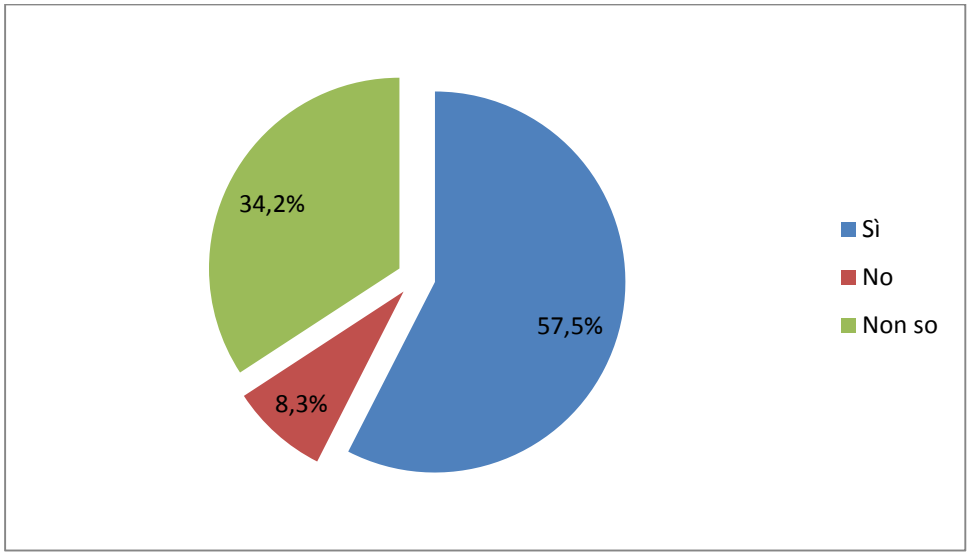
[diverse app accedono all'account di posta elettronica e alla rubrica nonché al microfono e alla videocamera degli smartphone e/o tablet?]"



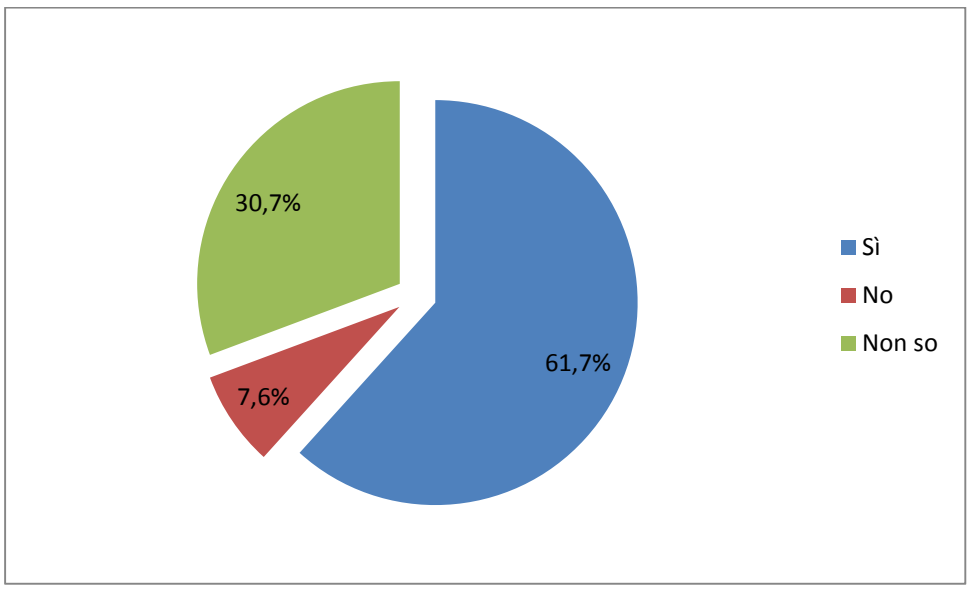
11. Infine, in circa 6 casi su 10 gli intervistati hanno dichiarato di essere a conoscenza del fatto che i loro dati costituiscono una fonte di guadagno per le imprese che li raccolgono e utilizzano (domanda 1.5, 57,5% degli intervistati) e una risorsa per l'attività

di analisi e previsione dei comportamenti degli utenti a scopi commerciali e non (domanda 1.6, 61,7% degli intervistati).

Domanda 1.5 – "Per quanto a sua conoscenza [l'utilizzo dei dati generati dalle attività su internet e dall'uso di smartphone e/o tablet da parte dei singoli utenti è fonte di guadagno per i soggetti che li raccolgono e/o utilizzano?]"



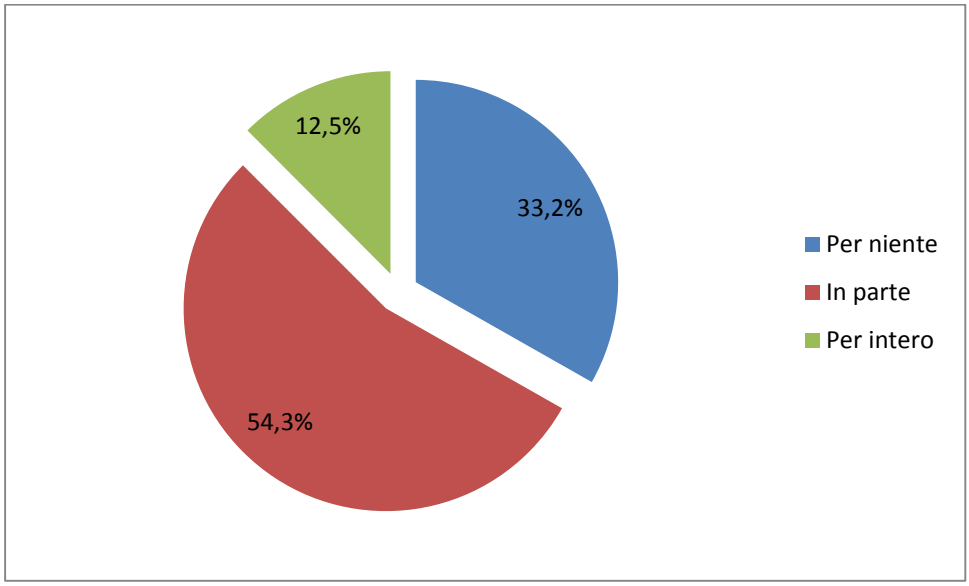
Domanda 1.6 – "Per quanto a sua conoscenza [i dati prodotti navigando su internet e utilizzando app e servizi online costituiscono una risorsa per i soggetti che realizzano analisi sui comportamenti degli utenti e per i soggetti che utilizzano tali analisi per fini pubblicitari e per altri scopi?]"



12. Un ulteriore set di domande ha quindi indagato quale sia l'approccio dei consumatori nei confronti delle informative per il consenso. La normativa europea e nazionale prevede infatti che, proprio in ragione della sensibilità ed ampiezza dei dati che possono essere raccolti nell'ambito dell'erogazione di servizi *online*, l'utilizzatore non solo sia adeguatamente informato circa il fatto che i suoi dati personali vengono raccolti e/o utilizzati, nonché gli scopi per cui tale raccolta viene effettuata, ma anche sia messo nella condizione di esprimere se acconsente o meno all'acquisizione, utilizzazione e cessione dei suoi dati. Tuttavia, all'atto di fruizione dei servizi *online* che comportano il rilascio di dati, il grado di tutela che tali norme intendono garantire potrebbe trovare un'attuazione solo parziale se gli utilizzatori non leggono il consenso o comunque dedicano a tale funzione un tempo inadeguato alla complessità del tema trattato, ovvero se le informative che ricevono risultano poco chiare.

13. Le risposte del campione evidenziano che la maggioranza degli utenti leggono solo in parte le informative (domanda 2, 54,3% degli intervistati) oppure non le leggono affatto (33,2%); solo una quota minoritaria degli intervistati (12,5%) dichiara di leggere per intero le informative.

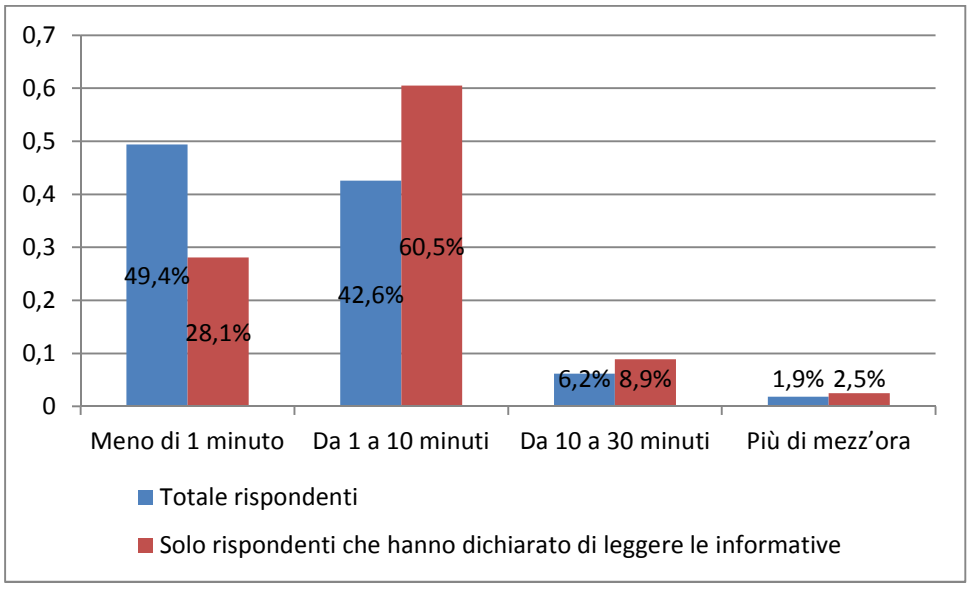
Domanda 2 – "Prima di decidere se concedere o negare il consenso all'acquisizione, utilizzazione e cessione dei suoi dati, Lei legge le relative informative?"



14. Le risposte relative al tempo in media dedicato alla lettura delle informative appaiono coerenti con quanto sopra evidenziato. Infatti, quasi la metà del campione di

utenti intervistati (compresi coloro che hanno dichiarato di non leggere affatto le informative) ha dichiarato di dedicare mediamente alla lettura meno di un minuto (domanda 3, 49,4%) e un'altra parte consistente ha dichiarato di dedicarvi fino a 10 minuti (42,6%)[7]. La circostanza per cui gli utenti *online* dedicano un arco temporale limitato alla lettura delle informative risulta confermata anche laddove si considerino solo gli intervistati che hanno dichiarato di leggere le informative (escludendo cioè coloro che hanno, al contrario, dichiarato di non leggerle affatto): anche in tale sottoinsieme, infatti, l'88,6% dedica fino a 10 minuti alla lettura delle informative (il 28,1% meno di un minuto, il 60,5% da uno a dieci minuti).

Domanda 3 - "Quanto tempo dedica in media alla lettura dell'informativa sull'acquisizione, utilizzazione e cessione dei dati?"



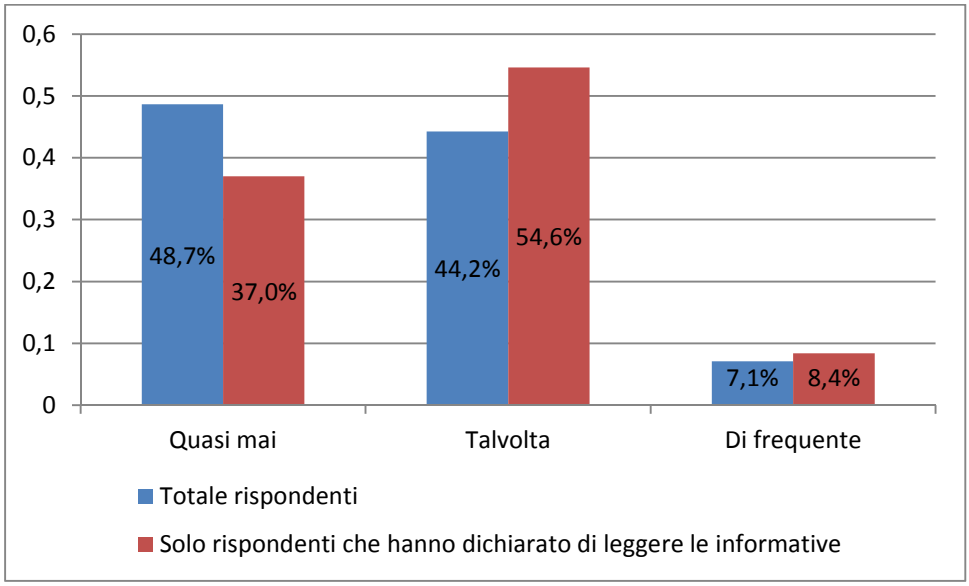
15. Agli utenti è stato altresì richiesto di esprimere la propria opinione circa la chiarezza delle informative per il consenso all'acquisizione, utilizzazione e cessione dei dati. La domanda è stata somministrata anche a coloro che hanno dichiarato di non leggere affatto le informative. Ciò in quanto la scarsa chiarezza delle informative potrebbe spiegare la decisione stessa di non leggerle e, pertanto, anche le risposte di

[7] Il 6,2% dei rispondenti dedica da 10 a 30 minuti alla lettura delle informative, l'1,9% vi dedica più di mezz'ora.

coloro che non leggono le informative può dare indicazioni circa il livello di comprensibilità delle stesse.

16. Dalle risposte del campione emerge che un'ampia maggioranza degli utenti ritiene che le informative risultino poco chiare. In particolare, le opinioni nettamente più diffuse tra tutti coloro che hanno risposto al questionario sono che il quadro informativo fornito sul tipo di dati acquisiti e sulle finalità del loro utilizzo è "quasi mai" chiaro (domanda 4, 48,7% degli intervistati) o solo "talvolta" chiaro (44,2%), mentre solo il 7,1% ritiene che il quadro informativo sia "di frequente" chiaro. Anche considerando solo le risposte di coloro che hanno dichiarato di leggere le informative (escludendo cioè coloro che hanno, al contrario, dichiarato di non leggerle affatto), l'opinione prevalente è che il quadro informativo fornito sul tipo di dati acquisiti e sulle finalità del loro utilizzo sia chiaro solo "talvolta" (54,6%) o "quasi mai" (37%); soltanto l'8,4% ritiene che le informazioni fornite "frequentemente" siano più chiare.

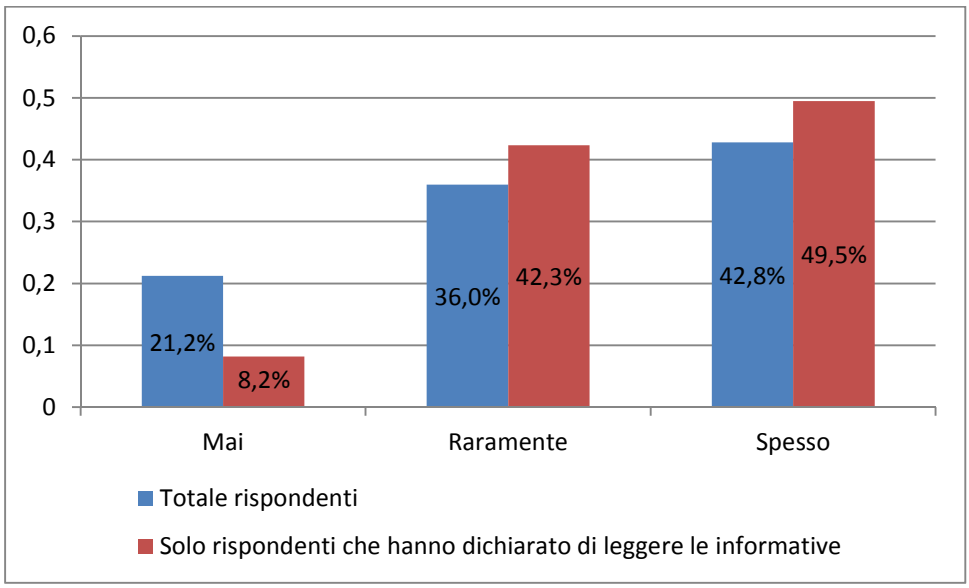
Domanda 4 - "Ritiene che le informative sull'acquisizione, utilizzazione e cessione dei dati forniscano un quadro chiaro sulla tipologia di dati che vengono raccolti e sulle finalità dell'utilizzo dei medesimi dati?"



17. Inoltre, a fronte della richiesta di valutare le proprie esperienze di lettura delle informative, gli intervistati si sono divisi in misura pressoché equa tra coloro che hanno dichiarato di essersi imbattuti "spesso" in informative poco chiare e coloro che dichiarano di aver fatto tale esperienza solo "raramente" o "mai". Le percentuali secondo cui si

sono ripartite le risposte risultano solo leggermente differenti a seconda che si consideri l'intero campione ovvero si escludano coloro che hanno dichiarato di non leggere affatto le informative (domanda 5). In particolare, il 42,8% degli utenti intervistati ha dichiarato che "spesso" è capitato loro di leggere informative poco chiare, mentre al 36% la medesima esperienza risulta essere capitata "raramente" ed al 21,2% "mai". Escludendo dal campione coloro che hanno dichiarato di non leggere affatto le informative, hanno letto "spesso" informative poco chiare il 49,5% degli utenti, "raramente" il 42,3%; solo l'8,2% dichiara di non aver "mai" letto informative poco chiare.

Domanda 5 - "Le è capitato di leggere delle informative sull'acquisizione, utilizzazione e cessione dei dati poco chiare?"



18. Le ragioni della scarsa chiarezza sembrano risiedere, in primo luogo, nella difficile comprensibilità del testo (50,9%) e nel carattere troppo piccolo con cui lo stesso viene riportato (50,1%). Seguono la descrizione non completa dei possibili utilizzi dei dati (31,4%), i rinvii a pagine difficilmente raggiungibili o leggibili (24%), la descrizione non completa dei dati acquisiti (22,8%) e il posizionamento dell'informativa nella schermata (14,4%)[8]. A queste motivazioni può aggiungersi l'eccessiva lunghezza del testo che risulta

[8] Tali esiti sono sostanzialmente confermati anche laddove non si considerino le risposte di coloro che hanno dichiarato di non leggere le informative: le risposte più frequenti sono la difficile comprensibilità del testo (50,4,%) e il carattere troppo piccolo del testo (49,3%), seguono la

essere la risposta più frequente tra quelle liberamente specificate dagli intervistati[9] (domanda 5-*bis*).

Domanda 5-bis – "Può specificare le cause della poca chiarezza riscontrata nell'informativa?"

Risposta	***Numero*** *(Intervistati che hanno indicato di aver letto "raramente" o "spesso" informative poco chiare)*	***Percentuale*** *(Intervistati che hanno indicato di aver letto "raramente" o "spesso" informative poco chiare)*	***Numero*** *(Esclusi intervistati che non leggono informative)*	***Percentuale*** *(Esclusi intervistati che non leggono informative)*
Testo scritto in un carattere piccolo	896	50,1	686	49,3
Posizionamento del testo all'interno della schermata	258	14,4	196	14,1
Rinvii a pagine o siti difficilmente raggiungibili o leggibili	428	24,0	361	25,9
Testo di difficile comprensione	909	50,9	702	50,4
Descrizione non completa della tipologia di dati acquisiti	408	22,8	338	24,3
Descrizione non completa dei possibili utilizzi dei dati	561	31,4	465	33,4
Altro	27	1,5	17	1,2
Totale	1787	100,0	1392	100,0

19. Le ultime domande di questa prima parte dell'indagine si sono incentrate sull'attitudine dei consumatori a fornire il consenso all'acquisizione, utilizzazione e cessione dei dati (domande 6 e 7 dell'indagine).

---

descrizione non completa dei possibili utilizzi dei dati (33,4%), rinvii a pagine difficilmente raggiungibili o leggibili (25,9%), descrizione non completa dei dati acquisiti (24,3%) e posizionamento dell'informativa nella schermata (14,1%)

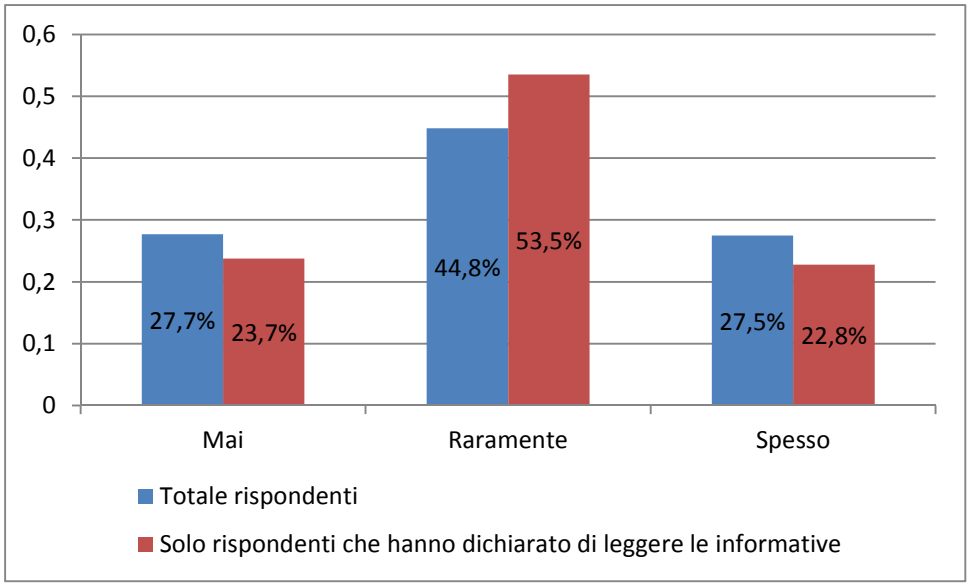
[9] Nello specifico, 24 rispondenti (17 se si escludono quelli che dichiarano di non leggere le informative) hanno indicato una risposta libera (valida) rimandando in 13 casi (6 nel gruppo più ristretto di rispondenti) all'eccessiva lunghezza dei testi.

20. A questo riguardo è emerso che anche utenti che non sono del tutto consapevoli della stretta relazione esistente tra cessione dei dati e gratuità del servizio, non di rado acconsentono all'acquisizione, utilizzazione e cessione dei propri dati personali. Ciò anche a fronte di informative ritenute poco chiare. In particolare, il 27,5% degli intervistati ha dichiarato di aver reso "spesso" il consenso all'acquisizione, utilizzazione ed eventuale cessione dei propri dati anche a fronte di informative poco chiare (la percentuale scende al 22,8% se si escludono le risposte fornite da coloro che hanno dichiarato di non leggere le informative). Pressoché analoghe sono le percentuali di coloro che, specularmente, non hanno reso "mai" il consenso (27,7% sull'intero campione e 23,7% sul sottoinsieme di coloro che hanno dichiarato di leggere le informative). La parte restante (44,8% dell'intero campione e 53,5% del sottoinsieme di coloro che hanno dichiarato di leggere le informative) lo ha reso "raramente (domanda 6.1).

Inoltre, circa i due terzi del campione hanno mostrato scarsa propensione a negare *tout court* il consenso (il 45,2% ha dichiarato di negarlo "raramente" ed il 21,5% di non negarlo "mai"). Solo un terzo del campione si è dichiarato propenso a negare "spesso" il consenso (33,4%, domanda 6.2).

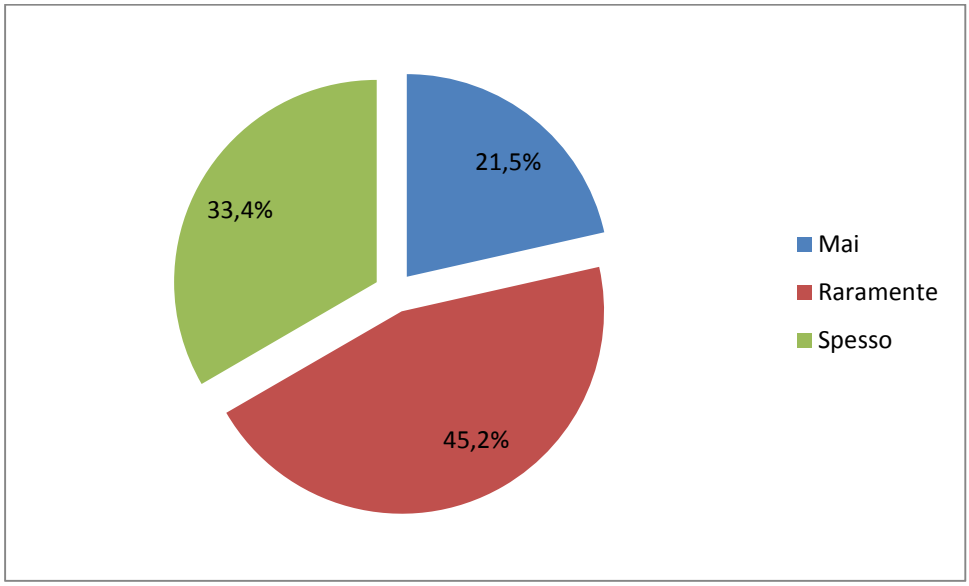
Domanda 6.1 – "Le è capitato di

[consentire all'acquisizione, utilizzazione e cessione dei dati malgrado la relativa informativa fosse poco chiara?]"



Domanda 6.2 - "Le è capitato di

[non consentire all'acquisizione, utilizzazione e cessione dei dati?]"



21. Gli utenti che negano il consenso lo fanno soprattutto in ragione dei timori di un improprio utilizzo dei propri dati: le preoccupazioni riguardano sia l'utilizzo a fini pubblicitari (46,7%) sia, ancor di più, l'utilizzo per altre finalità (50,2%) (cfr. domanda 7).

Domanda 7 - "Può specificare le cause che hanno portato a non consentire all'acquisizione, utilizzazione e cessione dei dati?"

Risposta	***Numero*** (Intervistati *che "raramente" o "spesso" hanno negato il consenso)*	***Percentuale*** (Intervistati *che "raramente" o "spesso" hanno negato il consenso)*
Scarsa chiarezza dell'informativa	680	38,2
Incompletezza dell'informativa	297	16,7
Preoccupazione per l'utilizzo dei suoi dati a fini pubblicitari	833	46,7
Preoccupazione per l'uso dei suoi dati a fini diversi dalla comunicazione pubblicitaria	894	50,2
Altro	14	0,8
Totale	1782	100,0

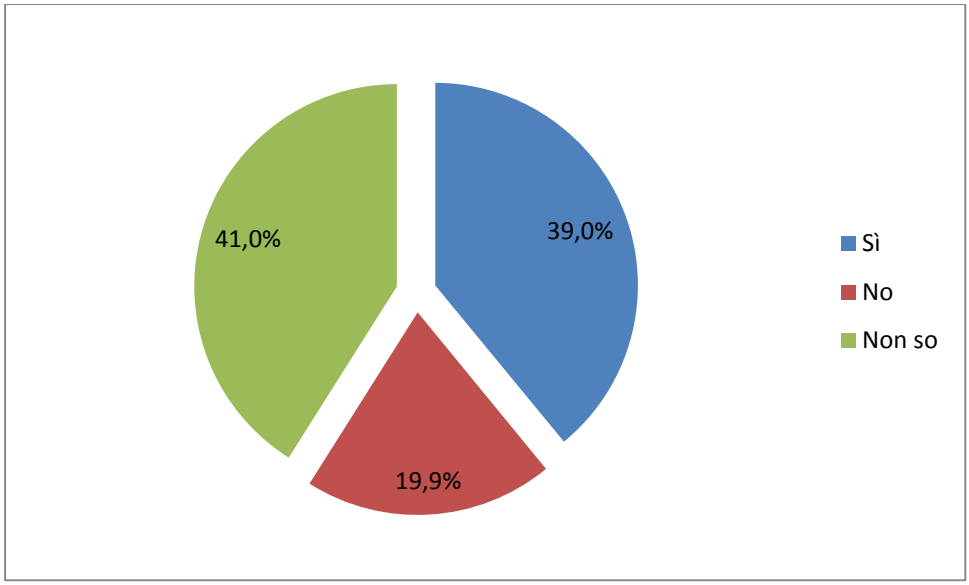
III. La disponibilità degli utenti a cedere i propri dati personali come forma di pagamento dei servizi online

22. La seconda parte dell'indagine si è incentrata sull'attitudine degli utilizzatori delle piattaforme *online* nei riguardi del rapporto tra fruizione dei servizi e cessione dei propri dati personali. Infatti, dal punto di vista economico, la condizione di ignoranza in cui si trovano gli utilizzatori di servizi *online* – i quali, scambiando un servizio con dati ceduti a prezzo nullo, non sono nella condizione di valutare se i benefici attesi dall'acquisto saranno proporzionati al suo costo[10] - rappresenta un fattore cruciale nell'analisi dei mercati dell'economia digitale, giacché in essa può radicarsi una esternalità positiva che dà luogo ad un eccessivo trasferimento di dati dai consumatori alle imprese.
Sotto questo profilo le domande da 8 a 15 hanno sondato quale sia la consapevolezza dei consumatori riguardo al fatto che l'utilizzo dei servizi offerti a prezzo nullo invero li coinvolge in una forma di scambio in cui sono proprio i dati a fungere da valuta, nonché la loro capacità di apprezzare il valore dei dati personali in relazione a quello dei servizi con i quali vengono scambiati.

23 Per quanto riguarda la consapevolezza degli utenti sul fatto che, di norma, il consenso all'acquisizione, utilizzazione e cessione dei dati costituisce condizione necessaria per poter usufruire gratuitamente di applicazioni e servizi *online* (domanda 8), dalle risposte del campione è emerso che 4 utenti su 10 sono consapevoli della stretta relazione esistente tra la concessione del consenso e la gratuità del servizio. Per contro, solo il 20% degli utenti sono convinti che non sussista alcuna relazione, mentre il 41% mostra di non averne consapevolezza.

[10] All'interno di una comune transazione economica in cui un soggetto acquista tra un bene o servizio in cambio di una determinata somma di denaro è infatti proprio il prezzo pagato che rende il consumatore consapevole della convenienza dello scambio.

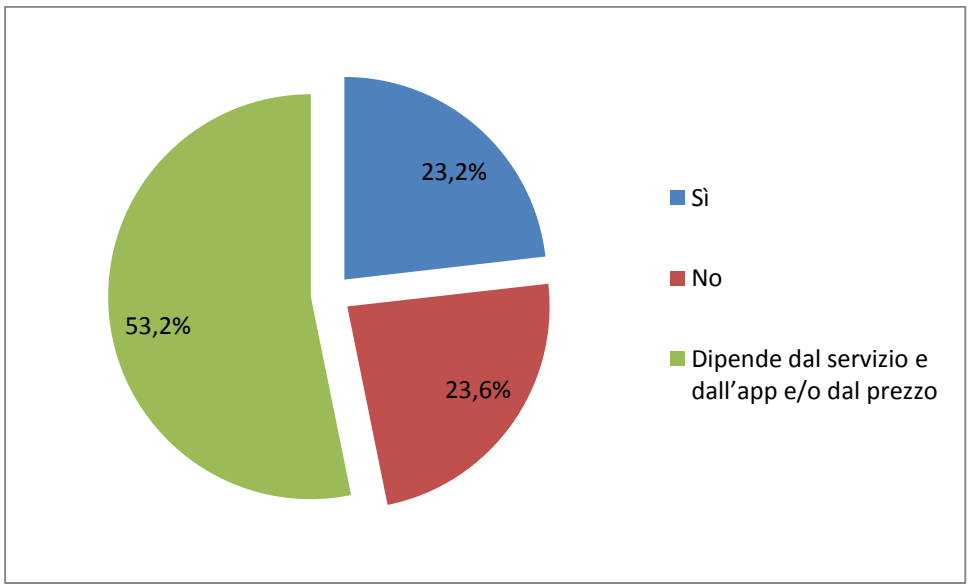
Domanda 8 – "Per quanto a sua conoscenza la concessione del consenso all'acquisizione, utilizzazione e cessione dei dati è condizione necessaria per poter usufruire di servizi e app gratuiti?"



24 L'indagine prosegue quindi con un approfondimento sul valore che gli utenti attribuiscono ai propri dati (domanda 9) nonché sulla loro effettiva disponibilità a pagare per ottenere i servizi *online* evitando o limitando il consenso all'acquisizione, utilizzazione e cessione dei propri dati (domande 10 e 11).

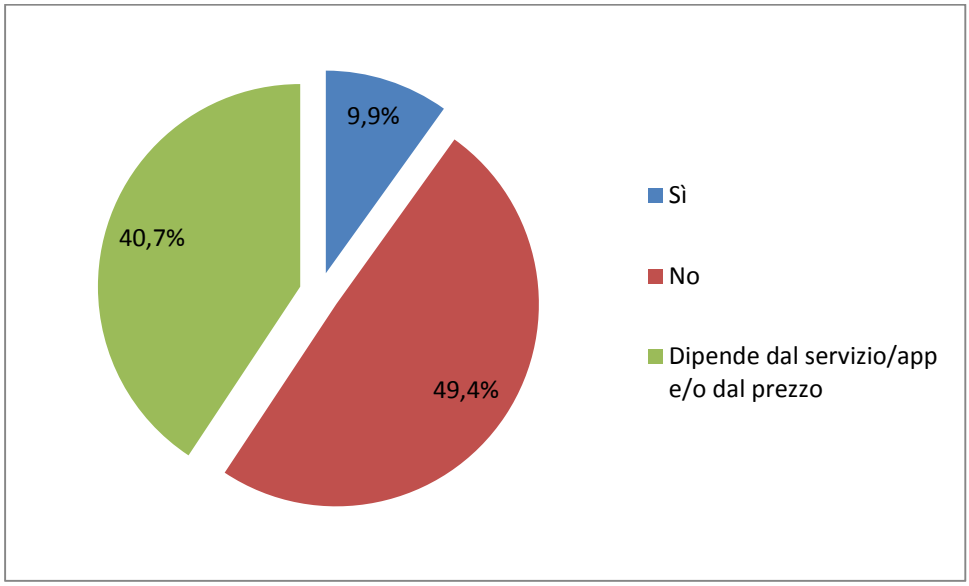
25 Dalle risposte del campione è emerso che oltre 3/4 degli utenti (76,4%, domanda 9) sarebbero disposti a rinunciare ai servizi e alle applicazioni gratuite per evitare che i propri dati siano acquisiti, elaborati ed eventualmente ceduti (segnatamente, il 23,2% degli intervistati ha risposto che sarebbe disponibile a rinunciare *tout court*, mentre per il 53,2% la disponibilità a rinunciare dipende dal servizio e/o dal prezzo eventualmente richiesto). Solo circa un utente su quattro (23,6%) ha risposto che non sarebbe disposta a rinunciare a servizi *online* di cui oggi usufruisce gratuitamente per evitare la raccolta dei propri dati.

Domanda 9 – "Sarebbe disposto a rinunciare ai servizi e *app* gratuiti per evitare che i suoi dati vengano acquisiti, elaborati ed eventualmente ceduti?"

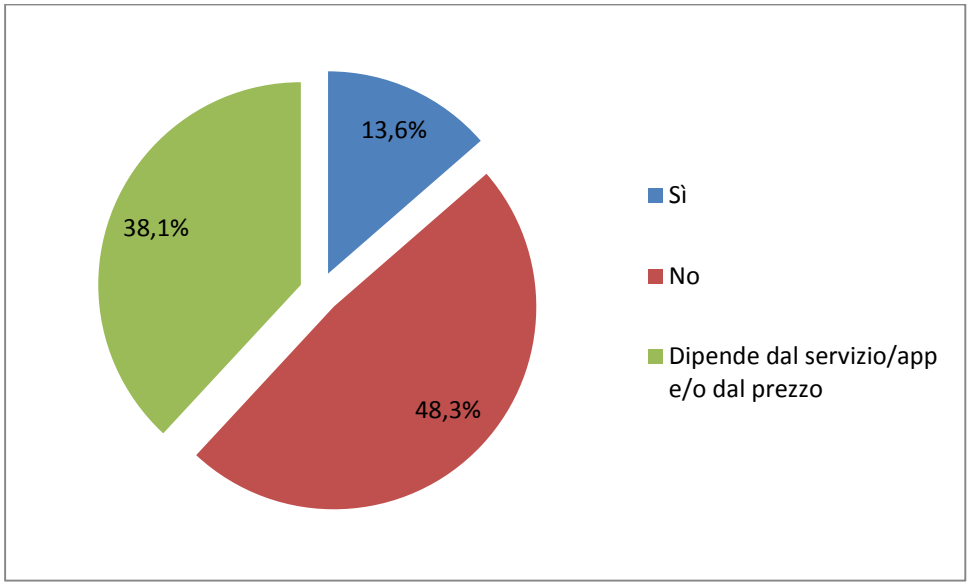


26 A fronte di ciò, è emersa tuttavia una bassa disponibilità, da parte degli utenti, a pagare per ottenere servizi/*app* oggi forniti gratuitamente così da evitare l'utilizzo dei propri dati: solo 1 utente su 10 sarebbe disposto a pagare per evitare lo sfruttamento pubblicitario dei propri dati (cfr. domanda 10.1); una percentuale maggiore (13,6%) sarebbe invece disposta a pagare per evitare lo sfruttamento dei propri dati per ulteriori finalità non specificate (cfr. domanda 10.2). In entrambi i casi, quasi il 50% degli utenti ha dichiarato di non avere nessuna disponibilità a pagare per i servizi oggi forniti gratuitamente, mentre la parte restante prenderebbe in considerazione questa eventualità valutando caso per caso in base al servizio in questione (segnatamente, il 40,7% la prenderebbe in considerazione per evitare lo sfruttamento pubblicitario dei propri dati ed il 38,1% per evitare altre forme non specificate di sfruttamento pubblicitario dei dati).

Domanda 10.1 – "Sarebbe disposto a pagare per servizi/app oggi gratuiti [per evitare che i suoi dati vengano raccolti e utilizzati per fini commerciali?]"



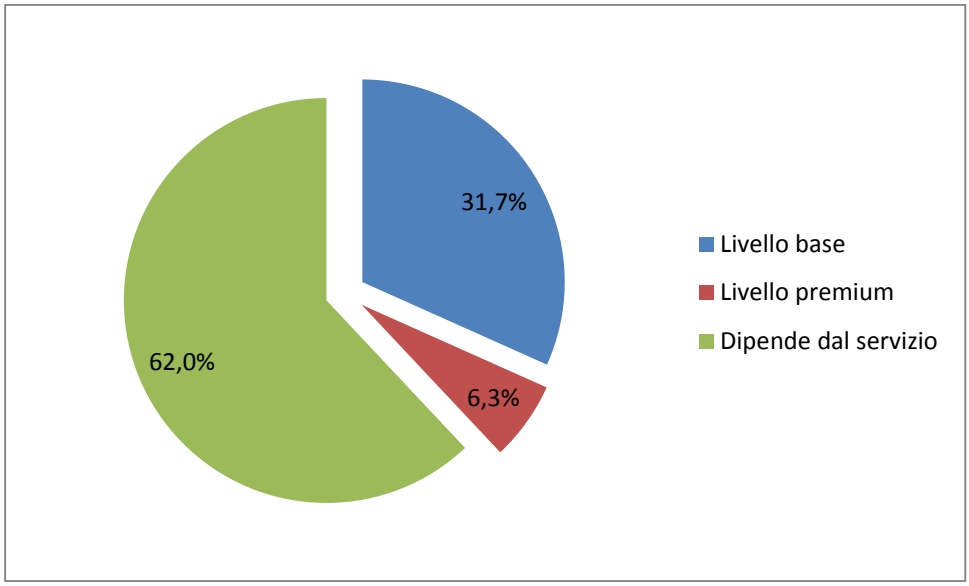
Domanda 10.2 – "Sarebbe disposto a pagare per servizi/app oggi gratuiti [per evitare che i suoi dati vengano raccolti e utilizzati per scopi diversi da quelli commerciali, ma non specificati?]"



27. Inoltre, dalle risposte alla domanda 11 è emerso che, a fronte di un ipotetico *trade-off* tra la qualità del servizio di cui fruire (servizio base in luogo di un servizio *premium*) e l'ampiezza del consenso all'acquisizione, utilizzazione e cessione dei propri dati, poco meno di un terzo degli intervistati sarebbe in ogni caso disponibile a fruire

soltanto di un servizio base pur di circoscrivere il consenso ad un sottoinsieme limitato di dati. Il 62% effettuerebbe tale valutazione caso per caso, in base alla tipologia del servizio, mentre il 6% acconsentirebbe all'utilizzo dei propri dati senza limitazioni pur di accedere ad un servizio *premium*.

Domanda 11 - "Se fosse possibile scegliere tra un servizio base (ad esempio, e-mail, social network, app, siti di informazione, piattaforme di contenuti musicali e audiovisivi, motori di ricerca) consentendo all'acquisizione, utilizzazione e cessione di un insieme limitato di dati e un servizio "premium" consentendo all'acquisizione, utilizzazione e cessione del complesso dei suoi dati, quale livello di servizio sceglierebbe?"



28. Concludono quindi la seconda parte dell'indagine una serie di domande (da 12 a 15) volte a verificare se un parametro idoneo per la misurazione del valore dei dati (dal punto di vista degli utenti) possa essere rappresentato dal fastidio per i messaggi pubblicitari o per i suggerimenti mostrati sui *device* e durante la navigazione in *internet*.

29. Dalle risposte alla domanda 13 è emerso che, benché gli utilizzatori trovino mediamente fastidiosi i messaggi pubblicitari, ciò non si traduce in una disponibilità a pagare per evitare le comunicazioni pubblicitarie. In particolare, in una scala da estremamente fastidioso (1) a estremamente utile (10), i messaggi pubblicitari sono ritenuti mediamente fastidiosi: la valutazione media è 4; più della metà del campione

(54%) ha manifestato fastidio (valori compresi tra 1 e 4) con una chiara prevalenza per il giudizio "estremamente fastidioso" (30,6%)[11]; un terzo (33,3%) ritiene che la pubblicità sia utile (valore tra 5 e 7)[12], la restante parte (12,7%) che sia molto utile (valori da 8 a 10).

A fronte di tali valutazioni, la maggioranza degli intervistati (56%) si dichiara tuttavia non disponibile a pagare per evitare che le vengano mostrati messaggi pubblicitari; per il 40,5% la disponibilità a pagare dipende dallo specifico servizio e dal prezzo (eventualmente) richiesto; solo una quota minoritaria (3,5%) si dichiara disponibile a pagare *tout court*.

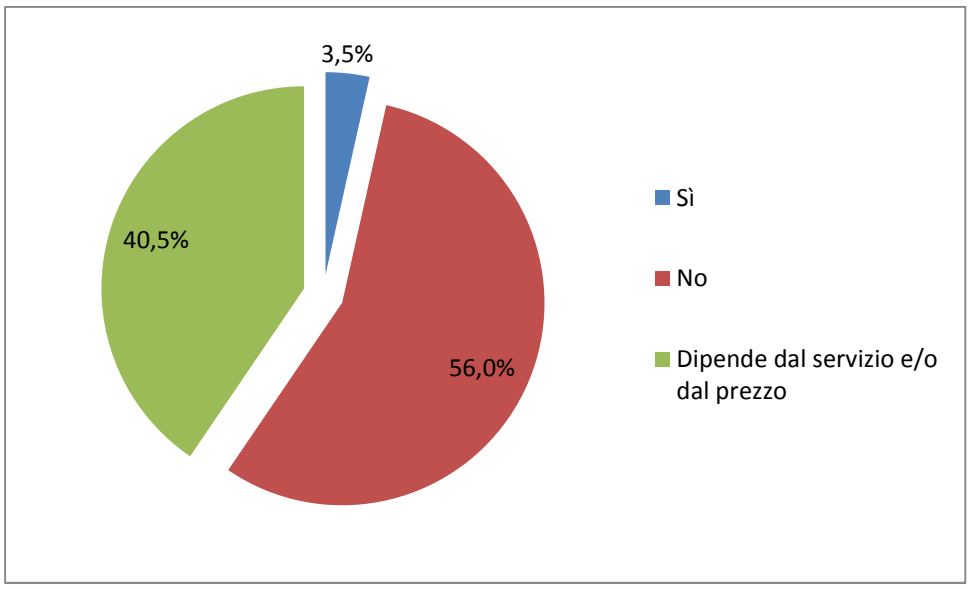
Domanda 12 – "In una scala da 1 a 10, dove 1 è estremamente fastidioso e 10 è estremamente utile, come giudica i messaggi pubblicitari che le vengono mostrati sul suo smartphone e/o tablet e durante la navigazione in internet?"

Risposta	***Numero***	***Percentuale***
1	694	30,6
2	215	9,5
3	167	7,4
4	149	6,6
5	291	12,8
6	310	13,7
7	155	6,8
8	107	4,7
9	57	2,5
10	124	5,5
Totale	2269	100,0
Media	4,07	
Dev. Standard	2,80	

[11] Questa risulta essere la risposta più frequente alla domanda 12.

[12] I valori 6 e 5, corrispondenti ad una valutazione di utilità, rappresentano la seconda e terza risposta più frequente, rispettivamente con il 13,7% e con il 12,8%. Considerate congiuntamente (26,5%), tali risposte risultano comunque meno frequenti di quella corrispondente a "estremamente fastidioso" (valore 1, 30,6%).

Domanda 13 – "Sarebbe disposto a pagare per evitare che le vengano mostrati messaggi pubblicitari sul suo smartphone e/o tablet e durante la navigazione in internet?"



30. Allo stesso modo, dalle risposte del campione è emerso che i suggerimenti mostrati sui *device* e durante la navigazione in *internet* sono considerati poco utili dagli utenti, i quali escludono nettamente di essere disposti a pagare per ottenere che tali suggerimenti siano loro mostrati (domanda 15.1). Tuttavia, gli stessi utilizzatori non mostrano di avere disponibilità a pagare neppure per evitare che detti suggerimenti vengano loro proposti. In particolare, secondo le risposte alla domanda 14, in una scala da estremamente fastidioso (1) a estremamente utile (10) i suggerimenti sono ritenuti mediamente poco utili o addirittura fastidiosi: la valutazione media è 4,2; quasi la metà del campione (49,6%) ha espresso valutazioni di fastidio o scarsa rilevanza (valori compresi tra 1 e 4) e la risposta più frequente è "estremamente fastidioso" (25,7%)[13]; il 40,5% attribuisce un'utilità ai suggerimenti (valori tra 5 e 7)[14], la restante parte (9,9%) ritiene i suggerimenti molto utili (valori da 8 a 10).

[13] Questa risulta essere la risposta più frequente alla domanda 14.

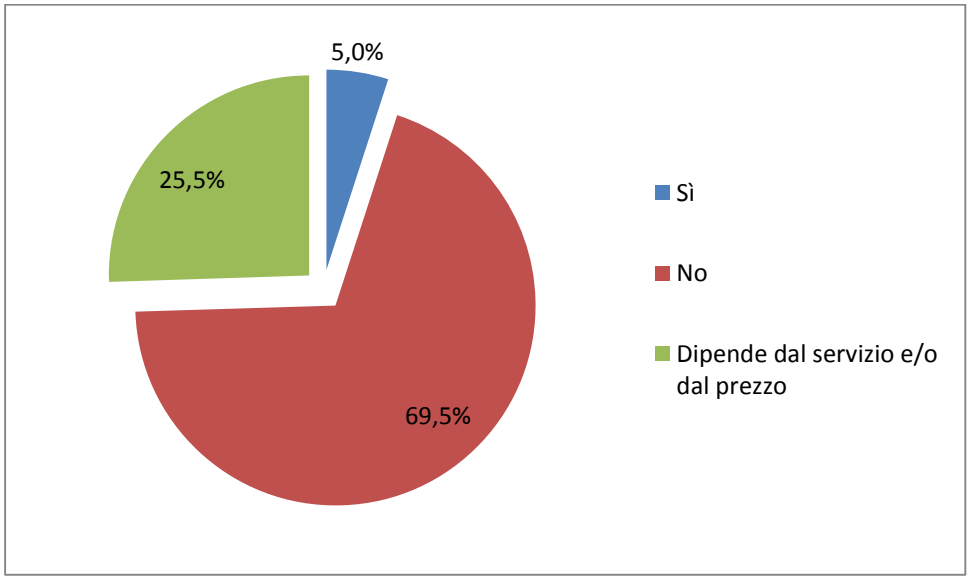
[14] I valori 5 e 6, corrispondenti ad una valutazione di utilità, rappresentano la seconda e terza risposta più frequente, rispettivamente con il 18,2% e con il 14,3%. Considerate congiuntamente (32,5%), tali risposte risultano più frequenti di quella corrispondente a "estremamente fastidioso" (valore 1, 25,7%).

A fronte di tali valutazioni, la larga maggioranza degli intervistati si dichiara non disponibile a pagare né per ottenere che vengano mostrati i suggerimenti (domanda 15.1, 69,5% "no") né per evitare che vengano mostrati (domanda 15.2, 60,7% "no"); una parte degli intervistati fa dipendere dallo specifico servizio o dal prezzo (eventualmente) richiesto la disponibilità a pagare per ottenere i suggerimenti (domanda 15.1, 25,5% "dipende") o al contrario per evitarli (domanda 15.2, 31,4% "dipende"); la disponibilità a pagare *tout court* risulta minoritaria (5% e 7,9%).

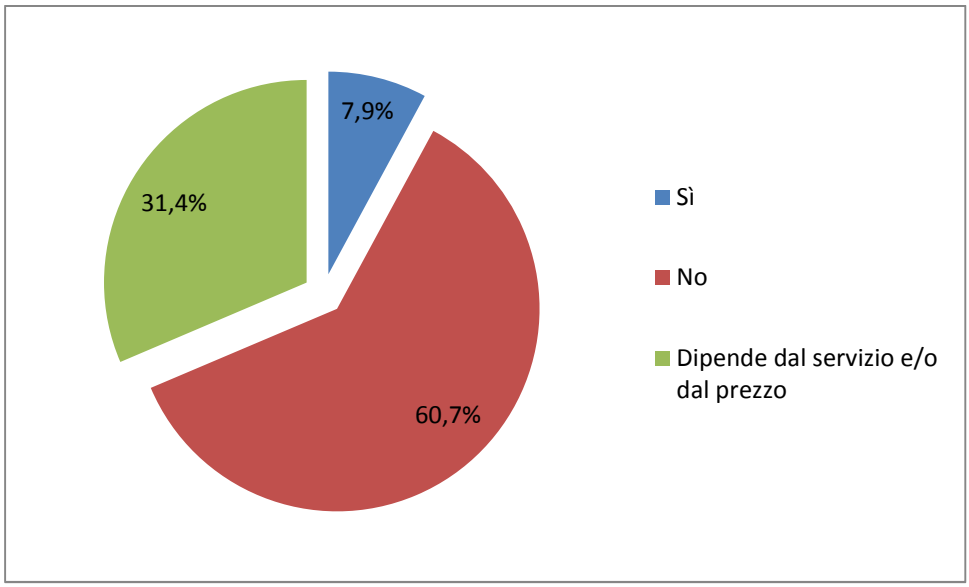
Domanda 14 – "In una scala da 1 a 10, dove 1 è estremamente fastidioso e 10 è estremamente utile, come giudica i suggerimenti (ad esempio, relativi ai contenuti musicali e audiovisivi o alle persone che potrebbe conoscere) che le vengono mostrati sul suo smartphone e/o tablet e durante la navigazione in internet?"

Risposta	*Numero*	*Percentuale*
1	584	25,7
2	173	7,6
3	201	8,9
4	167	7,4
5	413	18,2
6	325	14,3
7	182	8,0
8	117	5,2
9	41	1,8
10	66	2,9
Totale	2269	100,0
Media	4,17	
Dev. Standard	2,55	

Domanda 15.1 – "Sarebbe disposto a pagare per [ottenere che le vengano mostrati tali suggerimenti?]"



Domanda 15.2 – "Sarebbe disposto a pagare per [evitare che le vengano mostrati tali suggerimenti?]"



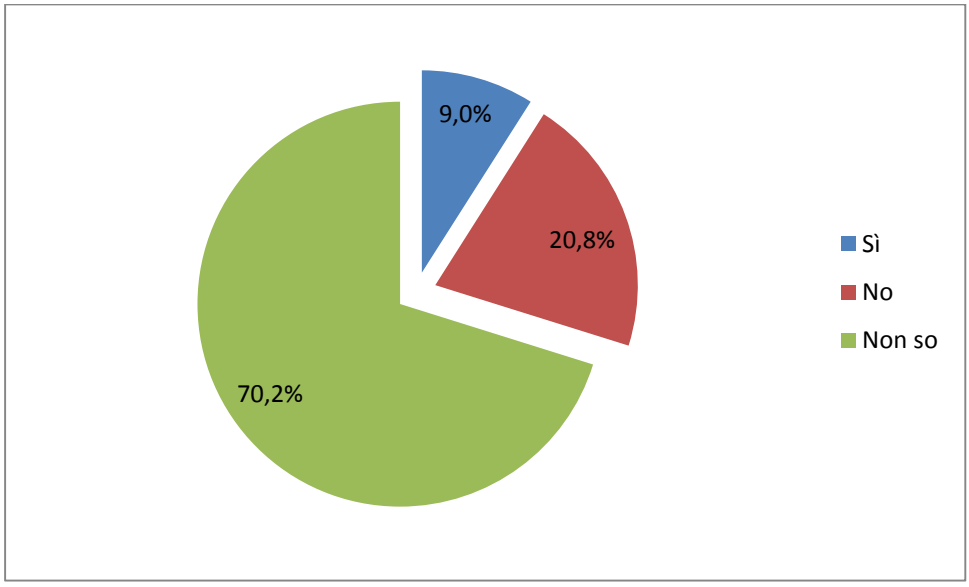
IV. La portabilità dei dati da una piattaforma all'altra

31. L'ultima parte dell'indagine si è focalizzata sulla attitudine dei consumatori nei riguardi della portabilità dei dati da una piattaforma all'altra, di recente introdotta dal

Regolamento UE 2016/679 (cosiddetto GDPR, General Data Protection Regulation) entrato in vigore lo scorso 25 maggio. Si tratta infatti di un elemento di particolare rilievo dal punto di vista della concorrenza, in quanto potenzialmente idoneo a ridurre gli *switching costs* che derivano dalla incapacità dei consumatori di avere il controllo sui dati ceduti e di usufruirne in caso di bisogno e, per tale via, ad accrescere la contendibilità dei mercati.

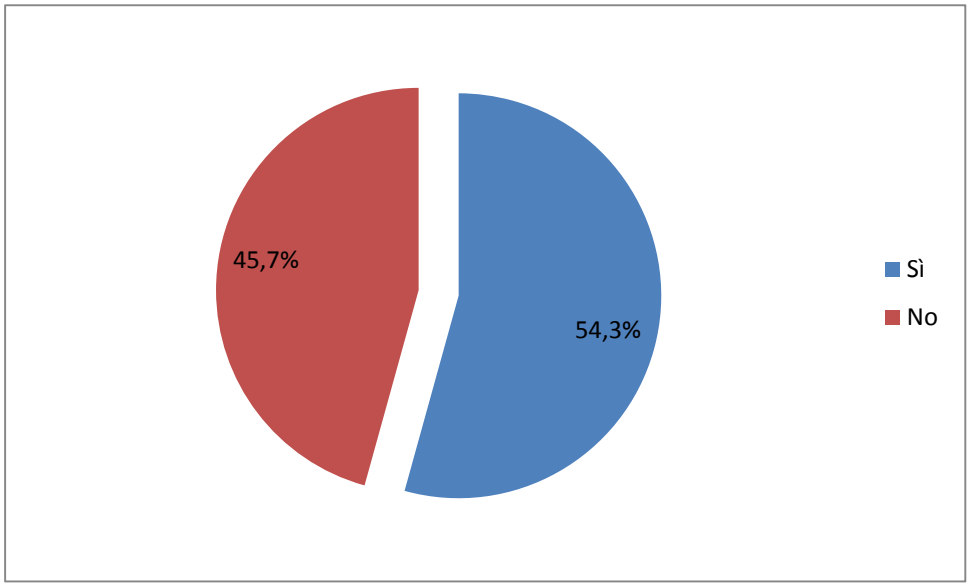
32. Dalle risposte del campione alla domanda 16 è emerso che, al momento dell'indagine, la maggior parte degli utenti non era a conoscenza della possibilità di scaricare i propri dati, conferiti in una piattaforma/applicazione *online*, ed eventualmente trasferirli ad un altro operatore: solo il 9% degli intervistati è risultato a conoscenza di tale diritto mentre il 91% lo ignorava (70,1% "non so", 20,9% "no").

Domanda 16 – "Per quanto a sua conoscenza, sarà generalizzata la possibilità per i singoli utenti di chiedere alle piattaforme e alle applicazioni una copia dei relativi dati sui comportamenti online per conservarla o anche trasferirla ad altre piattaforme/applicazioni?"



33. A fronte di ciò, poco più della meta degli utilizzatori intervistati si è dichiarata interessata ad ottenere una copia dei propri dati (54,3%, domanda 17).

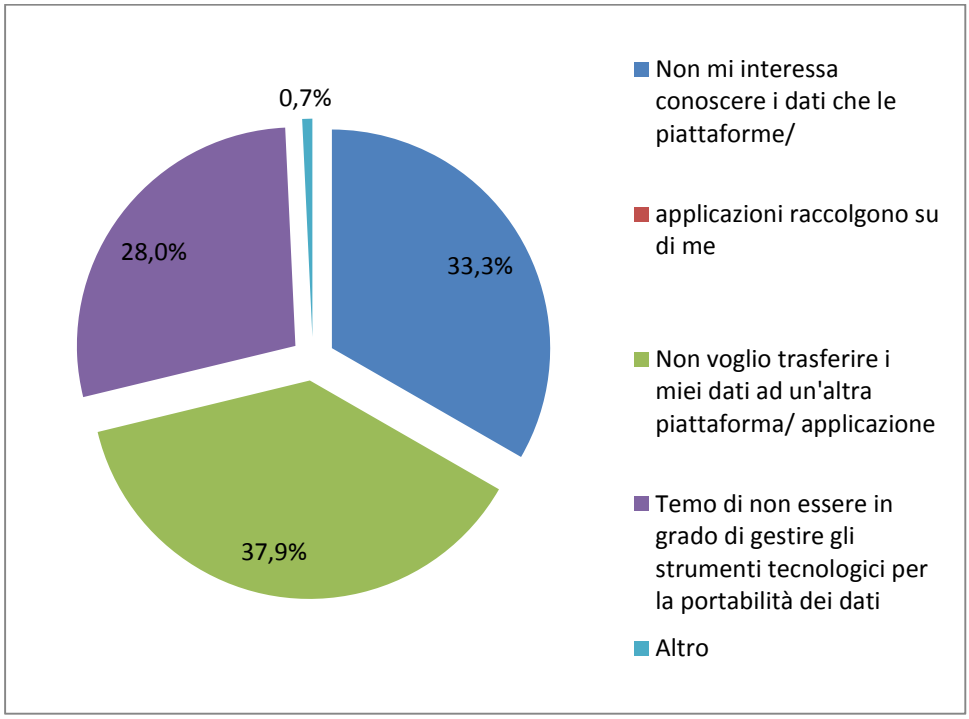
Domanda 17 – "Sarebbe interessato ad ottenere una copia dei suoi dati?"



34. La mancanza di interesse ad ottenere una copia dei propri dati, che è emersa dal 45,7% degli intervistati, è riconducibile alla indisponibilità a trasferire i propri dati ad un'altra piattaforma/applicazione (domanda 18[15] 41,1%), al disinteresse per i dati che vengono raccolti (36,1%) e al timore di non essere in grado di gestire gli strumenti tecnologici per la portabilità dei dati (30,4%).

[15] La domanda è stata somministrata soltanto a coloro che si sono dichiarati non interessati ad ottenere una copia dei propri dati (1.037 rispondenti).

Domanda 18 – "Per quale/i motivo/i non sarebbe interessato ad ottenere una copia dei suoi dati?"



V. Appendice

Composizione del campione di rispondenti per sesso

	Numero	*Percentuale*
Maschio	1074	47,3
Femmina	1195	52,7

Composizione del campione di rispondenti per classe di età

	Numero	*Percentuale*
16 - 24	262	11,5
25 - 34	233	10,3
35 - 44	415	18,3
45 - 54	551	24,3
55 - 64	407	17,9
65 +	401	17,7

Composizione del campione di rispondenti per area geografica

	Numero	*Percentuale*
Nord - Ovest	594	26,2
Nord - Est	393	17,3
Centro	383	16,9
Sud + Isole	899	39,6

Composizione del campione di rispondenti per titolo di studio

	Numero	*Percentuale*
Nessuno / Licenza Elementare	69	3,0
Licenza Media Inferiore	517	22,8
Diploma di Scuola Media Superiore	1215	53,5
Laurea / Master / Dottorato	468	20,6

Composizione del campione di rispondenti per professione

	Numero	*Percentuale*
Imprenditori/Professionisti/Dirigenti/proprietari e redditieri	125	5,5
Insegnanti/Giornalisti/artisti	100	4,4
Impiegati/Quadri	528	23,3
Negozianti, commercianti, artigiani	69	3,0
Operai specializzati e qualificati	159	7,0
Operai comuni, manovali, braccianti	64	2,8
Agricoltori conduttori	4	0,2
Agenti di commercio/Rappresentanti e lavoratori autonomi in genere	50	2,2
Casalinghe	261	11,5
Pensionati	390	17,2
Studenti	261	11,5
Altre condizioni professionali (militari, religiosi, ecc...)	79	3,5
Disoccupati o altre condizioni non professionali	179	7,9

Composizione del campione di rispondenti per numero di componenti del nucleo famigliare

	Numero	*Percentuale*
Monocomponente	151	6,7
2 componenti	590	26,0
3 componenti	620	27,3
4 componenti	697	30,7
5 o più componenti	211	9,3

BIG DATA
INDAGINE CONOSCITIVA CONGIUNTA
LINEE GUIDA E RACCOMANDAZIONI DI POLICY

Luglio 2019

In data 30 maggio 2017, l'Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni e il Garante per la protezione dei dati personali hanno avviato congiuntamente un'Indagine Conoscitiva per meglio comprendere le implicazioni per la privacy, la regolazione, la tutela del consumatore e l'antitrust, dello sviluppo dell'economia digitale e, in particolare, del fenomeno dei Big Data.

La disponibilità dei dati è infatti sempre più rilevante per l'ottimizzazione di processi e decisioni, per l'innovazione e per l'efficiente funzionamento dei mercati e i Big Data rappresentano un fenomeno che non è limitato a specifici settori ma investe l'economia nel suo complesso. Inoltre, lo sviluppo dell'economia data driven ha implicazioni non solo sul funzionamento dei mercati e sul benessere dei consumatori, ma anche sotto il profilo sociale e democratico. Le nuove forme in cui si manifesta il potere di mercato meritano, dunque, un'attenta valutazione per le implicazioni economiche e sociali che possono avere.

La decisione di privilegiare un approfondimento interdisciplinare e di svolgere un'Indagine Conoscitiva congiunta origina dalla piena consapevolezza che le caratteristiche dell'economia digitale sono molto spesso tali per cui gli obiettivi propri delle tre Autorità tendono quasi inevitabilmente ad intrecciarsi e non sempre sono agevolmente distinguibili. Laddove i rapporti non univoci tra concorrenza, privacy e pluralismo richiedono un coordinamento particolarmente stretto, il confronto costante tra le diverse autorità di garanzia si rende necessario anche al fine di riconoscere e riconciliare possibili trade-off tra strumenti e obiettivi delle diverse autorità.
Il contributo che ciascuna Autorità, nel rispetto delle proprie competenze, può offrire alle altre due risulta estremamente prezioso, sia per una migliore comprensione dei fenomeni in atto, sia per la scelta della strumentazione più appropriata per fronteggiare alcune specifiche criticità al confine tra le diverse competenze, sia, infine, per integrare gli interventi dell'autorità competente e meglio "posizionata".

Nel corso dell'Indagine sono state svolte circa quaranta audizioni, da parte delle diverse Autorità, nel cui ambito sono stati interpellati i principali operatori dell'economia dei dati, delle telecomunicazioni, dei settori finanziari e dell'editoria, nonché esperti e accademici; sono state inviate richieste di informazioni ai grandi operatori digitali e sono pervenuti numerosi contributi. Inoltre, le diverse Autorità hanno potuto beneficiare delle informazioni acquisite nel corso di procedimenti collegati allo sfruttamento economico dei dati e al ruolo della profilazione algoritmica nei mercati della pubblicità on line e nell'attività delle piattaforme di video sharing, motori di ricerca e marketplace.

Nel giugno dello scorso anno sono stati pubblicati alcuni risultati intermedi: un Big Data Interim report adottato dall'AGCom e un rapporto che illustra i risultati di un'indagine campionaria, condotta

dall'AGCM, volta a indagare la propensione degli utenti di servizi on-line a consentire l'utilizzo dei propri dati a fronte dell'erogazione dei servizi.

Il documento finale, che raccoglierà i rapporti finali delle diverse Autorità, sarà disponibile a breve.

Di seguito si anticipano le principali linee guida di cooperazione sul tema, nonché le raccomandazioni di policy condivise dalle tre autorità.

1.	*Governo e Parlamento si interroghino sulla necessità di promuovere un appropriato quadro normativo che affronti la questione della piena ed effettiva trasparenza nell'uso delle informazioni personali (nei confronti dei singoli e della collettività).*
2.	*Rafforzare la cooperazione internazionale sul disegno di policy per il governo dei Big Data.*
3.	*Promuovere una policy unica e trasparente circa l'estrazione, l'accessibilità e l'utilizzo dei dati pubblici al fine della determinazione di politiche pubbliche a vantaggio di imprese e cittadini. Sarà necessario un coordinamento tra tale policy e le strategie europee già esistenti per la costituzione di un mercato unico digitale.*
4.	*Ridurre le asimmetrie informative tra utenti e operatori digitali, nella fase di raccolta dei dati, nonché tra le grandi piattaforme digitali e gli altri operatori che di tali piattaforme si avvalgono.*
5.	*Prima delle operazioni di trattamento dei dati, identificare la loro natura e proprietà e valutare la possibilità d'identificazione della persona a partire da dati 'anonimizzati'.*
6.	*Introdurre nuovi strumenti per la promozione del pluralismo on-line, la trasparenza nella selezione dei contenuti nonché la consapevolezza degli utenti circa i contenuti e le informazioni ricevute on-line.*
7.	*Perseguire l'obiettivo di tutela del benessere del consumatore con l'ausilio degli strumenti propri del diritto antitrust estendendoli anche alla valutazione di obiettivi relativi alla qualità dei servizi, all'innovazione e all'equità.*
8.	*Riformare il controllo delle operazioni di concentrazioni al fine di aumentare l'efficacia dell'intervento delle autorità di concorrenza.*
9.	*Agevolare la portabilità e la mobilità di dati tra diverse piattaforme, tramite l'adozione di standard aperti e interoperabili*
10.	*Rafforzare i poteri di acquisizione delle informazioni da parte di AGCM ed AGCom al di fuori dei procedimenti istruttori e aumento del massimo edittale per le sanzioni al fine di garantire un efficace effetto deterrente delle norme a tutela del consumatore.*
11.	*Istituzione di un "coordinamento permanente" tra le tre Autorità.*

LINEE GUIDA E RACCOMANDAZIONI DI POLICY

1.	*Governo e Parlamento si interroghino sulla necessità di promuovere un appropriato quadro normativo che affronti la questione della piena ed effettiva trasparenza nell'uso delle informazioni personali (nei confronti dei singoli e della collettività).*

L'utilizzo intensivo dei *Big Data* costituisce un fenomeno che interessa sempre più l'intera economia e società. Agli indubbi vantaggi in termini di riduzione dei costi di transazione per imprese e cittadini-consumatori, si affiancano nuovi rischi sotto il profilo concorrenziale, della protezione del dato personale e del pluralismo informativo.

In particolare, la disponibilità in capo ai grandi operatori digitali, attivi su scala globale, di enormi volumi e varietà di dati (personali e non personali, strutturati e non strutturati) e della capacità di analizzarli ed elaborarli ha dato luogo a inedite forme di sfruttamento economico del dato e della sua valorizzazione ai fini della profilazione algoritmica legata a diversi scopi commerciali, generando nuove concentrazioni di potere, inteso non solo come 'potere di mercato', ma più in generale come potere economico e potere *tout court*, interessando i diritti fondamentali, i profili concorrenziali, il pluralismo e la stessa tenuta dei sistemi democratici. Si tratta pertanto di un fenomeno che merita attenzione da parte di tutte le istituzioni che contribuiscono a definire la *governance* dei mercati.

L'attuale assetto istituzionale è sostanzialmente adeguato a tutelare i diritti fondamentali, e in particolare il diritto alla protezione dei dati personali, e la concorrenza. Più complesso appare il tema della protezione del pluralismo informativo nella moderna società digitale, in ragione di nuove dinamiche che, diversamente dagli approcci tradizionali al pluralismo, volti a disciplinare forme di accesso dal lato dell'offerta ai media tradizionali, sembrano riguardare, invece, i comportamenti degli utenti dal lato della domanda, in un quadro di *overload* informativo e di limitata trasparenza circa l'origine delle informazioni e la loro natura editoriale, nonché circa gli effetti della profilazione sulla selezione dei contenuti proposti agli utenti.

Considerato il dinamismo e la complessità tecnica che caratterizzano gli ambiti presi in considerazione, Governo e Parlamento hanno la responsabilità di assicurare lo sviluppo equilibrato della cd. economia digitale nel rispetto dei diritti e delle libertà fondamentali, nonché di interrogarsi sulla necessità di promuovere un appropriato quadro normativo che affronti la questione della piena ed effettiva trasparenza e liceità nell'uso dei dati personali.

2.	*Rafforzare la cooperazione internazionale sul disegno di policy per il governo dei Big Data.*

La crescente interdipendenza dei mercati e di sistemi economici fa sì che le questioni sollevate dall'economia dei dati assumano spesso carattere sovra-nazionale.

Pertanto, in questo scenario nuovo ed evolutivo, un coordinamento fra le autorità della concorrenza europee non è solo auspicabile, ma necessario. A livello europeo, l'AGCM ha aderito alla Rete Europea della Concorrenza (*European Competition Network* - ECN), che riunisce la Commissione europea e le autorità *antitrust* istituite in ogni Stato Membro dell'Unione Europea, competenti ad applicare le regole di concorrenza stabilite dal TFUE. In particolare, nell'ambito dell'ECN, è stato costituito un gruppo di lavoro, denominato "*ECN Digital Markets",* ove le Autorità europee espongono le attività in corso in merito all'applicazione delle regole di concorrenza relative ad operatori digitali. La costituzione di tale gruppo di lavoro è volta, da un lato, a promuovere la cooperazione tra le autorità degli Stati Membri, d'altro lato, a favorire la corretta allocazione di procedimenti istruttori riguardanti

l'economia digitale. Inoltre, proprio anche in ragione della rapida evoluzione dei mercati digitali, è stata emanata la Direttiva UE 2019/1 (anche denominata ECN+) che conferisce alle autorità garanti della concorrenza degli Stati Membri poteri di applicazione più efficaci. Il dialogo transfrontaliero europeo non è soltanto legato a temi di concorrenza ma vi è anche un coordinamento interdisciplinare. Infatti, l'AGCM partecipa alla *Digital Clearing House*, istituita su iniziativa dello *European Data Protection Supervisor* (EDPS) per valutare le implicazioni dei *Big Data* sotto il profilo della tutela del consumatore, della concorrenza e della protezione dei dati personali. In ambito extra europeo, la cooperazione multilaterale tra autorità Antitrust viene attuata in tre sedi principali: l'Organismo per la Cooperazione e lo Sviluppo Economico (OCSE), l'*International Competition Network* (ICN) e il *United Nations Conference on Trade and Development* (UNCTAD).

Sotto un diverso angolo visuale, nella misura in cui un trattamento di dati personali posto in essere mediante tecniche di *Big Data* ha natura transfrontaliera, trova invece piena applicazione la disciplina di protezione dei dati personali secondo il modello di cooperazione rafforzata tra autorità nazionali di protezione dei dati personali previsto dal Capo VII del RGPD (artt. 60 ss). Modalità ulteriori (ancorché meno stringenti) di cooperazione tra autorità di protezione dei dati possono altresì avere luogo, su scala globale, nell'ambito del *Global Privacy Enforcement Network* – GPEN.

Sotto il profilo regolamentare, l'Autorità per le Garanzie nelle Comunicazioni partecipa attivamente all'analisi del BEREC sulla Economia dei dati (*Data Economy*), finalizzata a conoscere l'impatto della economia dei dati sui mercati delle comunicazioni elettroniche, nonché quale ruolo possano avere i servizi di comunicazione elettronica per lo sviluppo della economia dei dati, ed, infine, in quale misura le autorità nazionali di regolazione (ANR) possano trarre vantaggio dall'economia dei dati nello svolgimento delle attività istituzionali. In questo contesto, il BEREC si prefigge di stimolare la collaborazione tra le ANR al fine di valutare in qual modo l'esperienza regolamentare fin qui acquisita possa rivelarsi utile per affrontare le possibili problematiche competitive connesse allo sviluppo della economia dei dati. In particolare, assume rilevanza il ruolo del BEREC nel tracciare le linee guida per le ANR sui temi della neutralità della rete che vanno aggiornati al fine di tener conto, oltre al ruolo dei prezzi espliciti (nelle pratiche di cosiddetto *zero rating*), anche dello scambio implicito di servizi a fronte del rilascio di permessi circa l'uso del dato personale laddove tale pratica venisse associata a forme di discriminazione nell'erogazione di medesimi servizi agli utenti. Appare inoltre necessario, sempre in ambito BEREC, affrontare il tema della proprietà dei dati generati nel contesto delle connessioni 5G e oggetto di scambio tra imprese attive in settori oggetto di regolazione distinta (energia, comunicazioni elettroniche, trasporti, sanità ecc.), nonché il tema associato della standardizzazione del dato e al fine di favorire l'interoperabilità dei servizi offerti.
Infine, anche AGCom partecipa alla *Digital Clearing House* dell'Unione Europea, in cui si esaminano le problematiche dei *Big Data*, con riguardo ad aspetti di interesse per tutte e tre le Autorità.

3.	*Promuovere una policy unica e trasparente circa l'estrazione, l'accessibilità e l'utilizzo dei dati pubblici al fine della determinazione di politiche pubbliche a vantaggio di imprese e cittadini. Sarà necessario un coordinamento tra tale policy e le strategie europee già esistenti per la costituzione di un mercato unico digitale.*

Il ricorso ai *Big Data* in modo crescente interessa trattamenti ulteriori rispetto a quelli effettuati mediante reti di comunicazioni elettronica ovvero nel settore privato, estendendosi ai trattamenti da parte di soggetti pubblici nel perseguimento di finalità istituzionali.

Anche tali soggetti, i quali peraltro originariamente acquisiscono le informazioni personali finalizzate all'assolvimento della propria missione istituzionale sulla base di obblighi legali gravanti sugli

interessati, devono assicurarsi che il ricorso alle tecniche *Big Data*, anche con l'ausilio dei responsabili della protezione dei dati (Rpd), avvenga nel rispetto delle discipline di protezione dei dati personali.

4.	*Ridurre le asimmetrie informative tra utenti e operatori digitali, nella fase di raccolta dei dati, nonché tra le grandi piattaforme digitali e gli altri operatori che di tali piattaforme si avvalgono.*

La riduzione dell'asimmetria informativa tra utenti e operatori digitali nella fase di raccolta dei dati costituisce un fondamentale obiettivo di *policy* al quale possono e devono contribuire diversi strumenti. In questo quadro appare rilevante informare compiutamente l'utente-consumatore non solo circa gli usi dei dati ceduti, ma anche circa la necessità della cessione in merito al funzionamento del servizio offerto. Il rapporto *interim* dell'AGCom ha evidenziato come molte *app* mostrino una relazione inversa tra prezzo di acquisto dell'*app* e permessi richiesti all'utente, talvolta anche per la medesima *app*. Appare indispensabile che l'utente, nelle decisioni di acquisto del servizio e di cessione del dato abbia piena consapevolezza della relazione tra permessi necessari al funzionamento dell'*app* e permessi ulteriori richiesti a seguito di cessione del dato.

Sia l'applicazione della normativa sulla protezione dei dati personali che la strumentazione propria della tutela del consumatore possono offrire un contributo importante per la riduzione di tale asimmetria informativa, garantendo che gli utenti ricevano un'adeguata, puntuale e immediata informazione circa le finalità della raccolta e dell'utilizzo dei loro dati e siano posti nella condizione di esercitare consapevolmente ed effettivamente le proprie scelte di consumo. In questa prospettiva, appaiono opportune misure volte a rendere maggiormente consapevoli i consumatori nel momento in cui forniscono il consenso al trattamento dei loro dati personali.

Appare altresì ineludibile che si proceda ad una progressiva riduzione delle asimmetrie informative tra le grandi piattaforme digitali e gli altri operatori che si avvalgono di tali piattaforme, aumentando la trasparenza dei criteri con i quali i dati vengono analizzati ed elaborati (ad esempio, nella definizione del *ranking* relativo al posizionamento e alla visibilità sulla piattaforma) e favorendo l'ingresso di nuovi intermediari dei dati che, su mandato degli utenti e nel rispetto della normativa a tutela della *privacy*, possano interfacciarsi con le grandi piattaforme globali con un accresciuto potere negoziale in merito alla contrattazione sul valore del dato e sul suo impiego commerciale.

In ogni caso, si avverte la necessità (non solo nello scenario nazionale) che le autorità di controllo siano messe in condizione di dotarsi di adeguati profili professionali (i cd. *data scientist*) per garantire l'adempimento dei propri compiti istituzionali.

5.	*Prima delle operazioni di trattamento dei dati, identificare la loro natura e proprietà e valutare la possibilità d'identificazione della persona a partire da dati 'anonimizzati'.*

Appare necessario che chi intenda effettuare operazioni di trattamento secondo la metodologia propria dei *Big Data* si accerti, in via preliminare, della natura personale o meno dei dati trattati, così da identificare la cornice normativa di riferimento all'interno della quale opera.

Inoltre, i titolari del trattamento che intendono far uso di *Big Data* dovrebbero preventivamente valutare se una persona possa essere ragionevolmente identificata a partire dalla serie di dati "anonimizzata" utilizzata nel corso dell'analisi, in ragione delle operazioni di trattamento effettuate e

dei *dataset* impiegati. Ciò non solo nell'ottica di rafforzamento della sicurezza del trattamento dei dati personali, come già previsto dal RGPD, ma anche nell'ottica di coerenza con la strategia nazionale di sicurezza cibernetica.

6.	*Introdurre nuovi strumenti per la promozione del pluralismo on-line, la trasparenza nella selezione dei contenuti nonché la consapevolezza degli utenti circa i contenuti e le informazioni ricevute on-line.*

La concorrenza è senza dubbio uno strumento utile, ma insufficiente, per garantire la tutela del pluralismo. Anche un processo competitivo funzionante può, infatti, portare ad assetti di mercato incoerenti con un'informazione effettivamente pluralistica, in presenza di strategie di disinformazione nonché di fenomeni di autoselezione informativa, particolarmente diffusi nei comportamenti *on-line*, come il pregiudizio di conferma (*confirmation bias*), l'ancoraggio alle prime impressioni (*anchoring effect*), le camere d'eco (*echo chamber*), il conformismo di gruppo (*groupthink effect*) e così via. In questi casi, la disponibilità di una pluralità di fonti informative, e quindi l'operare del meccanismo concorrenziale dal lato dell'offerta, potrebbe non essere sufficiente a generare informazione verificata di qualità, diversità e pluralismo, potendo produrre anzi, in taluni casi, forme accentuate di autoselezione e polarizzazione nella ricerca e nella diffusione di informazioni (*backfire effect*).

Negli ultimi anni sia la Commissione europea che l'AGCom hanno avviato un percorso di auto-regolazione e di co-regolamentazione che coinvolge tutte le componenti della società, ed in particolare tende a responsabilizzare le piattaforme tecnologiche, mediante l'adozione di appositi codici di comportamento volti a garantire sforzi concreti in favore della correttezza, completezza, verificabilità e non discriminatorietà dell'informazione accessibile *on-line*. Si tratta di un approccio distinto da quello tradizionalmente rivolto agli operatori media tradizionali in ragione della diversa natura di costruzione e diffusione dei contenuti, nonché della natura e della responsabilità editoriale degli stessi. Sul piano europeo, si ricorda il Piano d'adozione adottato a dicembre 2018 dalla Commissione europea per rafforzare la cooperazione tra Stati membri ed istituzioni europee, al fine di contrastare la crescente disinformazione che caratterizza il web e, tra le altre cose, condiziona negativamente la formazione del libero pensiero e le scelte del cittadino, in particolare, con riguardo alla formazione dell'orientamento politico ed all'espressione del voto.

Sul fronte delle iniziative dell'AGCom, si richiama in particolare il "*Tavolo per la garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali*" istituito nel novembre 2017, che ha l'obiettivo di favorire e promuovere l'autoregolamentazione delle piattaforme e lo scambio di buone prassi per l'individuazione ed il contrasto dei fenomeni di disinformazione *on-line* frutto di strategie mirate. L'iniziativa, peraltro, si inscrive nel percorso istituzionale intrapreso da AGCom già a partire dal 2015, con la pubblicazione di rapporti e indagini conoscitive sul sistema dell'informazione *on-line*.

Dall'esperienza AGCom emergono tuttavia alcuni evidenti limiti di forme di autoregolazione che non siano accompagnate da poteri di *audit* e di *inspection* circa il ruolo della profilazione algoritmica nella selezione dei contenuti. Risulta pertanto auspicabile una verifica terza e indipendente degli esiti e dell'impatto misurabile delle iniziative di autoregolazione. In questa prospettiva, sembrano opportune iniziative legislative volte ad assicurare alle autorità indipendenti preposte alla tutela del pluralismo, poteri di *audit* e di *inspection* circa la profilazione algoritmica ai fini della selezione delle informazioni e dei contenuti, nonché in relazione agli esiti dell'applicazione delle *policy* e delle regole che le piattaforme digitali globali si sono date in tema di rimozione di informazioni false o di *hatespeech*. Manca, infatti, ad oggi, una reportistica verificabile di tali autonome iniziative. Con riferimento, infine,

al tema delle espressioni d'odio (*hatespeech*), a seguito della trasposizione della nuova Direttiva sui servizi media audiovisivi, l'AGCom applicherà anche alle piattaforme di *videosharing* il proprio regolamento di cui alla Delibera 157/19/CONS, avviando nel frattempo forme di co-regolazione per questo tipo di piattaforme.

7.	*Perseguire l'obiettivo di tutela del benessere del consumatore con l'ausilio degli strumenti propri del diritto antitrust estendendoli anche alla valutazione di obiettivi relativi alla qualità dei servizi, all'innovazione e all'equità.*

Sotto il profilo dell'*enforcement* antitrust, la repressione di comportamenti abusivi da parte dei grandi *player* dell'economia digitale e di intese restrittive della concorrenza, entrambi facilitati dallo sviluppo di nuovi *software* e algoritmi sofisticati, è una delle priorità nell'attività dell'AGCM.

Le caratteristiche dell'economia digitale richiedono la ricerca di un nuovo equilibrio tra il rischio di scoraggiare i processi innovativi e il rischio di *under-enforcement*.

La capacità di profilazione, portata ai suoi estremi, e l'esasperazione degli effetti di rete possono agevolare comportamenti abusivi idonei a ridurre la contendibilità degli ecosistemi delle principali piattaforme, rendendo persistente il loro potere di mercato. In particolare, in ragione della natura multisettoriale dell'economia digitale e della presenza di grandi operatori digitali attivi su più mercati, la definizione del mercato rilevante ai fini dell'accertamento del potere di mercato potrebbe essere ripensata, talvolta tenendo significativamente in considerazione anche altri elementi.

In futuro la diffusione di algoritmi di prezzo pro-collusivi può facilitare la stabilità di cartelli e la creazione di contesti di mercato favorevoli ad equilibri collusivi.

L'AGCM intende prestare una particolare attenzione alle condotte delle piattaforme digitali che possono potenzialmente determinare effetti restrittivi della concorrenza, come dimostrano le istruttorie antitrust recentemente avviate.

In questa prospettiva, inoltre, per perseguire l'obiettivo di tutela del benessere del consumatore, diventa opportuno non confinare l'analisi ai tradizionali parametri legati a prezzi e quantità, ma, con l'ausilio degli strumenti propri del diritto *antitrust*, estenderla anche alla qualità, all'innovazione e all'equità.

Appaiono infine necessarie, quantomeno con riferimento alle piattaforme digitali globali, misure volte ad incrementare la trasparenza all'utente circa la natura della propria profilazione in merito ai contenuti ricevuti, nonché meccanismi di o*pt-in* circa il grado di profilazione prescelto, e ciò anche ai fini della tutela del pluralismo *on-line*, in relazione alla selezione dei contenuti operante attraverso la profilazione del consumatore.

8.	*Riformare il controllo delle operazioni di concentrazioni al fine di aumentare l'efficacia dell'intervento delle autorità di concorrenza.*

Con la diffusione dei *Big Data*, il controllo delle concentrazioni assume una nuova centralità. Al fine di aumentare l'efficacia dell'intervento delle autorità di concorrenza rispetto alle operazioni di concentrazione è auspicabile:

1. una riforma a livello nazionale e internazionale che consenta alle autorità di concorrenza di poter valutare pienamente anche quelle operazioni di concentrazione sotto le attuali soglie richieste per

la comunicazione preventiva, ma che potrebbero risultare idonee a restringere sin dalla loro nascita importanti forme di concorrenza potenziale (come le acquisizioni da parte dei grandi operatori digitali di *start-up* particolarmente innovative anche soprannominate '*killing acquisitions*');

2. la modifica dell'art. 6, comma 1, della legge n. 287/90, con l'introduzione di uno *standard* valutativo più adatto alle sfide dell'economia digitale, che faccia leva sul criterio dell'impedimento significativo della concorrenza effettiva (SIEC – "*Substantial impediment to effective competition*").

9.	*Agevolare la portabilità e la mobilità di dati tra diverse piattaforme, tramite l'adozione di standard aperti e interoperabili*

Agevolare la portabilità e la mobilità di dati tra diverse piattaforme, tramite l'adozione di standard aperti e interoperabili, anche oltre quanto già previsto dal diritto alla portabilità di cui all'art. 20 del RGPD, costituisce un obiettivo con una forte valenza pro-concorrenziale.

In casi particolari, ferma restando la necessità di tutelare il diritto alla protezione dei dati personali, la tutela della concorrenza potrebbe richiedere obblighi di mobilità e portabilità dei dati personali ulteriori rispetto a quelli previsti in generale dal RGPD.

A questo riguardo, si dovrebbe considerare la possibilità di estendere lo strumento della portabilità dei dati, oltre quanto – meritoriamente – stabilito dall'articolo 20 del RGPD, prevedendo una disciplina della portabilità dei dati, che favorisca lo sviluppo della competizione nei vari ambiti di valorizzazione economica del dato e, di conseguenza, una più efficace tutela del consumatore-utente. Possono pertanto essere prese in considerazione iniziative legislative o regolamentari, nell'ambito della cooperazione con l'Unione Europea, per disciplinare l'interoperabilità delle piattaforme tecnologiche, così da consentire effettivamente all'utente una piena portabilità dei propri dati.

10.	*Rafforzare i poteri di acquisizione delle informazioni da parte di AGCM ed AGCom al di fuori dei procedimenti istruttori e aumento del massimo edittale per le sanzioni al fine di garantire un efficace effetto deterrente delle norme a tutela del consumatore.*

La tutela del consumatore può intervenire su una molteplicità di profili connessi al rapporto tra operatori e utenti nella fase di acquisizione, elaborazione e trattamento dei dati. La circostanza che alle condotte poste in essere dalle imprese sia applicabile la normativa in materia di protezione dei dati personali non le esonera dal rispettare le norme in materia di pratiche commerciali scorrette, ponendosi le due discipline su un piano di complementarietà e non di alternatività. Le caratteristiche delle politiche di protezione dei consumatori e di tutela della *privacy* sono senza dubbio componenti importanti di un confronto concorrenziale *fair*.

Tenuto conto delle grandi dimensioni di molti operatori attivi nell'economia digitale, impregiudicato quanto già previsto dal RGPD, al fine di garantire un efficace effetto deterrente delle norme a tutela del consumatore, sembra necessario prevedere quanto prima un aumento del massimo edittale per le sanzioni.

Al fine di consentire una piena comprensione dei nuovi fenomeni in atto nell'economia digitale, appare opportuno il rafforzamento dei poteri di acquisizione delle informazioni da parte di AGCM ed AGCom al di fuori dei procedimenti istruttori (indagini conoscitive, attività pre-istruttoria), anche prevedendo la possibilità di irrogare sanzioni amministrative in caso di rifiuto o ritardo nel fornire le informazioni

richieste o in presenza di informazioni ingannevoli od omissive. In questa direzione è peraltro orientata la cornice normativa in materia di protezione dei dati personali (cfr. artt. 157 e 166, comma 2, del Codice in materia di protezione dei dati personali).

11. *Istituzione di un "coordinamento permanente" tra le tre Autorità.*

Un'efficace politica pubblica per i *Big Data* e l'economia digitale richiede non solo l'*enforcement*, ma anche un'adeguata attività di *advocacy* di cui l'iniziativa congiunta tra AGCM, AGCom e Garante per la protezione dei dati personali è testimonianza – volta a:

- contrastare le norme e le regolazioni volte a proteggere assetti di mercato "maturi" a scapito dello sviluppo delle innovazioni favorite dalla digitalizzazione, che contribuiscono alla competitività del sistema economico e al benessere dei consumatori;
- definire un *level playing field* attraverso misure volte alla rimozione degli ingiustificati vantaggi sotto il profilo fiscale e delle relazioni industriali di cui beneficiano i principali protagonisti della rivoluzione digitale in generale e in relazione ai diversi mercati rilevanti interessati e ai versanti intermediati dalle grandi piattaforme digitali;
- emancipare e accrescere la consapevolezza della collettività sia dei benefici che dei rischi derivanti dalla digitalizzazione dell'economia.

Con riguardo al tema specifico dell'accesso ai dati, le sinergie tra tutela della concorrenza e regolazione possono risultare preziose:

- ai sensi della normativa *antitrust*, un'impresa in posizione dominante può essere soggetta all'obbligo di fornire accesso ai dati indispensabili e non agevolmente duplicabili per salvaguardare la concorrenza in uno o più mercati in cui la medesima impresa è attiva;
- se invece l'obiettivo sociale è quello di tutelare interessi pubblici diversi dalla promozione della concorrenza, eventuali circoscritti interventi regolatori in materia di accesso ai dati appaiono più efficaci, così come possono contribuire alla promozione della concorrenza quando l'intervento *antitrust* si riveli insufficiente;
- in particolare, con riferimento alle competenze AGCom, sarà oggetto di valutazione quanto previsto dal nuovo codice europeo delle comunicazioni elettroniche di cui alla Direttiva UE 2018/1972 dell'11 dicembre 2018, laddove si specifica che "il trattamento dei dati personali da parte dei servizi di comunicazione elettronica, sia esso in forma di remunerazione o in altra forma, dovrebbe essere conforme al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio" (par. 15) e che "i servizi di comunicazione elettronica sono spesso forniti all'utente finale non solo in cambio di denaro, ma in misura sempre maggiore e in particolare in cambio della comunicazione di dati personali o di altri dati" concludendo che il concetto di remunerazione dovrebbe pertanto ricomprendere anche "le situazioni in cui l'utente finale è esposto a messaggi pubblicitari come condizione per l'accesso al servizio o le situazioni in cui il fornitore del servizio monetizza i dati personali raccolti in conformità del regolamento (UE) 2016/679" (par. 16);
- laddove l'accesso ai dati vada garantito nell'interesse generale, regolazioni settoriali che consentano allo Stato di accedere a banche dati raccolte da imprese private e utili per ragioni di salute pubblica, ambientali, di sicurezza o di mobilità, sembrano lo strumento più appropriato per garantire obiettivi di interesse pubblico ed evitare inutili e costose duplicazioni di dati già disponibili;

- l'accesso a taluni dati in possesso delle piattaforme digitali globali, e la loro replicabilità, può essere necessario anche per i soggetti preposti alla rilevazione delle 'audience', al fine di garantire lo sviluppo pro-concorrenziale dei mercati della pubblicità *on-line* - e del cosiddetto *programmatic advertising* basato sulla profilazione algoritmica degli utenti - e di assicurare un'equa ripartizione delle risorse idonea a promuovere un'offerta informativa di qualità;
- in ogni caso, eventuali interventi regolatori in materia di accesso ai dati devono essere necessari e proporzionati e devono tenere in considerazione le specificità del servizio/mercato al quale si riferiscono nonché le finalità sociali ad essi connesse e oggetto di presidio regolatorio;
- il contenuto di eventuali obblighi di accesso ai dati personali – in termini di ampiezza, natura e modalità – deve essere adeguatamente bilanciato con il diritto alla protezione dei dati personali.

Più in generale, le sfide poste dallo sviluppo dell'economia digitale e dai *Big Data* richiedono uno sfruttamento pieno delle sinergie esistenti tra strumentazione *ex ante* ed *ex post*, a tutela della *privacy*, della concorrenza, del consumatore e del pluralismo.

AGCM, AGCom e Garante per la protezione dei dati personali, ciascuno nell'ambito delle proprie competenze, possono meglio garantire i propri obiettivi istituzionali, nella misura in cui sapranno cogliere a pieno le opportunità offerte da una proficua cooperazione.

A tal fine, le tre Autorità, nell'esercizio delle competenze complementari ad esse assegnate e che contribuiscono a fronteggiare le criticità dell'economia digitale, si impegnano a strette forme di collaborazione negli interventi che interessano i mercati digitali, anche attraverso la sottoscrizione di un *memorandum of understanding*.