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.