TeLex Anie
NOVITÀ LEGISLATIVE E GIURISPRUDENZIALI

Segnalazioni giuridiche a cura del Servizio Centrale Legale

N. 1 Anno XXVIII
Gennaio 2023

INDICE:

CONCORRENZA

ABUSO DI POSIZIONE DOMINANTE E SETTORE FERROVIARIO – LA CGUE RESPINGE L'APPELLO PRESENTATO DALLA SOCIETÀ NAZIONALE DELLE FERROVIE LITUANE, CONFERMANDO UN APPROCCIO PIÙ SEVERO IN MATERIA DI ABUSI NEI CONFRONTI DI MONOPOLISTI LEGALI

Con la sentenza pubblicata lo scorso 12 gennaio (la *Sentenza*), la Corte di Giustizia dell'Unione europea (*CGUE*) – confermando l'approccio espresso dall'Avvocato Generale Rantos nelle sue conclusioni del 7 luglio 2022 – ha respinto integralmente l'appello presentato da Lietuvos geležinkeliai AB (***Lietuvos***), la società nazionale delle ferrovie della Lituania.
Lietuvos ha impugnato la sentenza con cui il Tribunale dell'Unione europea (il *Tribunale*) aveva confermato come quest'ultima avesse effettivamente abusato della propria posizione di dominanza nel mercato lituano del trasporto ferroviario di merci, così come precedentemente accertato dalla Commissione europea (la *Commissione*) nella decisione del 2 ottobre 2017 (la *Decisione*).
È utile brevemente ripercorrere i passaggi fattuali che hanno interessato la presente vicenda.

Con un accordo firmato nel 1999 la Lietuvos garantiva alla società L'Orlen Lietuva AB (***L'Orlen***) (congiuntamente con Lietuvos, le ***Parti***) – società lituana specializzata nella raffinazione di petrolio grezzo e nella distribuzione dei relativi prodotti – la fornitura di servizi di trasporto su rotaia dei suddetti prodotti sull'intero territorio lituano tramite la rete ferroviaria gestita da Lietuvos stessa. A seguito di una controversia intercorsa tra le Parti nel 2008, L'Orlen ha optato per una migrazione dei propri prodotti verso la vicina Lettonia e ha così deciso, a tal fine, di avvalersi dei servizi di trasporto forniti dalla società Latvijas dzelzceļš (*LDZ*), ossia la società nazionale delle ferrovie lettoni. Tuttavia, L'Orlen per potere trasportare i propri prodotti dalla Lituania alla Lettonia per fruire dei servizi offerti a condizioni più economiche da LDZ, avrebbe comunque dovuto continuare ad utilizzare una (seppur limitata) porzione di linea ferroviaria sita in Lituania e sotto il controllo di Lietuvos. Lietuvos, pochi mesi dopo che L'Orlen aveva preso contatti con LDZ, a valle di asseriti accertamenti che avevano individuato una deformazione su una decina di metri sui binari interessati, ha sospeso il traffico su tale tratto della linea e, circa un mese dopo, ha proceduto allo smantellamento fisico di 19 km della stessa senza mai avviare i lavori di manutenzione. A causa di tale smantellamento, L'Orlen non ha quindi potuto godere dei servizi offerti da LDZ. Tale condotta è stata oggetto di istruttoria da parte della Commissione, la quale aveva inflitto alla Lietuvos una sanzione di circa 28 milioni di euro per abuso di posizione dominante.
Lietuvos, in data 14 dicembre 2017, aveva quindi presentato ricorso avverso tale decisione dinnanzi al Tribunale, il quale tuttavia lo ha rigettato con la sentenza del 18 novembre riconoscendo la bontà della ricostruzione fattuale e giuridica operata dalla Commissione (benché abbia ridotto l'ammontare della sanzione imposta). Lietuvos ha successivamente presentato appello dinnanzi alla CGUE, basando le proprie argomentazioni su quattro motivi di appello: i primi tre atti a contestare la sussistenza di un abuso di posizione dominante; il quarto, invece, volto a contestare l'ammenda inflitta.

Il *focus* del presente commento è sui primi due motivi relativi alla contestata esistenza di una condotta abusiva.

In particolare, con il primo motivo, Lietuvos aveva sostenuto che il Tribunale avrebbe erroneamente mancato di applicare i criteri indicati dalla stessa CGUE nel caso *Bronner*, i quali regolano la c.d. *essential facility doctrine*, ossia che il rifiuto di concedere accesso a una infrastruttura essenziale costituisce una violazione dell'articolo 102 TFUE se **a)** detto rifiuto è idoneo ad eliminare qualsiasi concorrenza nel mercato rilevante, **b)** viene apposto in assenza di un'oggettiva giustificazione e **c)** tale accesso all'infrastruttura risulta indispensabile per l'esercizio dell'attività economica dell'impresa richiedente. Sul punto, la Sentenza – accogliendo quanto affermato dal Tribunale – sostiene che i succitati criteri non potessero trovare applicazione in relazione alla condotta posta in essere da Lietuvos, date le diverse premesse fattuali. Infatti, la CGUE ha indicato come il ragionamento di cui alla sentenza *Bronner*, pensata per società dominanti che non solo possiedono l'infrastruttura interessata ma l'hanno costruita con le proprie risorse e per i fini delle proprie attività commerciali, non trova applicazione in relazione a fattispecie – come quella in esame – in cui la dominanza derivi da un monopolio legale accompagnato da un obbligo di fornitura nei confronti dell'impresa dominante. Inoltre, la CGUE ha

sottolineato come la distruzione di parte dell'infrastruttura effettuata da Lietuvos non costituisce un "problema di accesso" ai sensi della sentenza *Bronner*, in quanto tale condotta implica il "*sacrificio di un attivo, con relativi costi"*: in seguito alla distruzione l'infrastruttura diviene inevitabilmente inutilizzabile non solo per il terzo richiedente ma anche per la stessa impresa dominante.
Per quanto qui rileva, Lietuvos sostiene altresì che il Tribunale avrebbe fondato la qualifica "abusiva" della condotta esclusivamente su due elementi cumulativi di per sé insufficienti e relativi al fatto che tale rimozione era stata effettuata: a) **"**precipitosamente*"*; e *b) "senza* [che Lietuvos avesse] *ottenuto preliminarmente i fondi necessari"* alla sostituzione del tratto interessato. La CGUE ha rigettato tale motivo sottolineando come il Tribunale – e quindi la Commissione – avesse accertato la natura abusiva della pratica in questione prendendo in esame una pluralità di elementi ulteriori ai due indicati da Lietuvos, come ad esempio il fatto che Lietuvos era a conoscenza del progetto di L'Orlen di reindirizzare le proprie attività verso la Lettonia e così avvalersi dei servizi di LDZ; che la rimozione sia stata effettuata senza previamente ottenere i fondi necessari alla sostituzione o adottare le normali misure preparatorie alla ricostruzione; che la rimozione del binario era in contrasto con la prassi corrente del settore; nonché del fatto che Lietuvos era perfettamente al corrente del rischio di perdere ogni attività di trasporto dei prodotti di L'Orlen in caso di ricostruzione del binario e che pertanto si era adoperata per convincere il governo lituano a non ricostruire il binario.

La CGUE ha posto così la parola fine alla vicenda iniziata ormai quasi sei anni fa, riconoscendo l'abusività della condotta posta in essere da Lietuvos.

La Sentenza, in particolare, dovrà essere tenuta in considerazione con riguardo all'affermazione dell'inapplicabilità dei criteri *Bronner* nel caso di società dominanti che godono di un monopolio legale e che usufruiscono di una cd. *essential facility* in relazione a cui esiste un obbligo normativo di garanzia di accesso.

Avv. Luca Feltrin
Freshfields Bruckhaus Deringer

OSSERVATORIO LEGISLAZIONE / GIURISPRUDENZA

CYBERSECURITY, SI RIPARTE: IMPRESE E GENERAZIONE Z ALLE PRESE CON NUOVE SFIDE ED OPPORTUNITÀ !

Premessa
A pochi anni dalla sua entrata in vigore, la Direttiva 2016/1148 (anche detta NIS, Network and Information Security Directive, di seguito la "Direttiva NIS") è già destinata ad un prepensionamento: il 28 novembre 2022 è stato infatti definitivamente licenziato il testo della Direttiva NIS 2 (di seguito anche solo la "Direttiva" o "NIS 2"), che la sostituirà introducendo un (nuovo) livello comune elevato di cibersicurezza nell'Unione.
Anche se dalla sua pubblicazione in Gazzetta gli Stati Membri avranno 21 mesi per conformarsi al nuovo regime, è consigliabile per le imprese che rientrino nell'ambito di applicazione della NIS 2 valutare con congruo anticipo le misure da adottare al fine di adeguare i propri presidi in tema di cybersecurity.

Criticità dell'attuale regime
La pandemia di questi ultimi anni ha mostrato quanto la società e l'economia siano – e saranno sempre più – pervase dalla digitalizzazione e vulnerabili agli attacchi degli hacker. La Direttiva NIS si è rivelata inadeguata, sia perché non abbraccia tutti i settori digitalizzati, sia perché non è sufficientemente chiara nel determinare il suo ambito di applicazione, lasciando agli Stati Membri ampia discrezionalità nell'individuazione dei soggetti sottoposti agli obblighi di adozione di misure di sicurezza e segnalazione degli incidenti: il che ha fatto sì che alcuni soggetti lo fossero in alcuni Paesi, ma non in altri.
È stato inoltre rilevato che - vigente la Direttiva NIS – gli Stati hanno mostrato riluttanza nell'applicazione di sanzioni ai soggetti che omettano di adottare requisiti di sicurezza o di segnalare incidenti [1]: con la conseguenza che l'impianto normativo previsto a livello comunitario è risultato, nella sua pratica attuazione, claudicante.

Il nuovo regime
a) **Ambito di applicazione** – Per far fronte ai problemi sopra evidenziati la Direttiva ha essa stessa previsto criteri dimensionali e qualitativi utili

ad individuare i soggetti cui si applica la disciplina sulla cybersecurity.

Cosicché, in linea di principio, gli obblighi previsti dalla NIS 2 graveranno anzitutto su tutte le **medie e grandi imprese** che operino nei settori individuati negli Allegati I [2] e II [3] della Direttiva: ma, **in presenza di certi requisiti** [4], il nuovo regime potrà trovare applicazione anche alle **piccole o microimprese**.

I destinatari del nuovo regime vengono quindi distinti in soggetti essenziali e soggetti importanti. Tra i primi ritroviamo anzitutto le grandi imprese operanti nei settori di cui all'Allegato I (con eccezione degli Enti della Pubblica Amministrazione), mentre tra i secondi le medie imprese operanti nei medesimi settori in cui operano i soggetti essenziali e le grandi e medie imprese che operano nei settori di cui all'Allegato II. Vi sono poi dei casi specifici, in cui l'appartenenza all'una o all'altra categoria di soggetti prescinde dalla dimensione: ad esempio, le medie imprese fornitrici di reti pubbliche di comunicazione elettronica o servizi di comunicazione elettronica accessibili al pubblico rientrano tra i soggetti essenziali, mentre le piccole e microimprese che offrano tali medesimi servizi sono da considerarsi soggetti importanti.

b) **obblighi** – I soggetti essenziali ed i soggetti importanti sono gravati dagli stessi obblighi, mentre differiscono quanto alla vigilanza, che viene esercitata – da parte degli organi statali preposti – sui primi ex ante e sui secondi ex post.

   Soggetti essenziali ed importanti devono quindi adottare misure tecniche e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nella fornitura dei loro servizi [5].

   L'obbligo investe, indirettamente, anche i **fornitori** (di servizi) dei soggetti essenziali ed importanti, rispetto ai quali vanno verificate, volta per volta, le specifiche vulnerabilità e la qualità complessiva dei prodotti e delle pratiche di cibersicurezza: conseguenza della amplificata interconnessione digitale e del fatto che i fornitori possono inconsapevolmente operare da cavalli di Troia e così veicolare attacchi cyber all'indirizzo del committente.

   Sempre indistintamente sui soggetti essenziali ed importanti grava l'**obbligo di notificare** senza indebito ritardo (e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente) – alle autorità competenti e/o a seconda dei casi ai destinatari stessi dei loro servizi – eventuali incidenti che abbiano un impatto significativo sulla fornitura dei loro servizi e qualunque minaccia informatica significativa capace di causare un incidente significativo [6].

   Per superare eventuali esitazioni, la Direttiva statuisce espressamente che l'assolvimento dell'obbligo di notifica non espone il soggetto notificante ad una maggiore responsabilità.

c) **governance** – La NIS 2 introduce un nuovo profilo di **responsabilità degli amministratori** dei soggetti essenziali e importanti. Questi devono infatti approvare le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti per conformarsi al nuovo regime e vigilare sull'attuazione delle stesse. Inoltre possono essere chiamati a rispondere in caso di mancato rispetto, da parte dei soggetti, di tali obblighi.

   Gli amministratori sono infine tenuti a seguire attività di formazione al fine di acquisire conoscenze e competenze sufficienti per comprendere e valutare i rischi di cibersicurezza e le relative pratiche di gestione e il loro impatto sulle attività del soggetto.

d) **sanzioni** – Viste le premesse, ci si sarebbe attesi indicazioni più puntuali circa il regime sanzionatorio applicabile in caso di violazioni delle norme sulla cybersecurity: al contrario, la NIS 2 si limita a ribadire quanto già stabilito nella Direttiva NIS invitando gli Stati Membri a prevedere (e, aggiungo, applicare) sanzioni effettive, proporzionate e dissuasive. C'è da sperare che gli Stati si mostrino meno titubanti nell'applicazione delle sanzioni, vista la posta in gioco.

Conclusioni

La NIS 2, una volta recepita, avrà importanti ripercussioni sulle imprese (che ricadano nella definizione di soggetti essenziali o importanti) e sui loro organi di gestione. È innegabile, d'altro canto, che – complice la trasformazione digitale in atto – le imprese (e non solo) sono oggi più esposte di quanto non lo fossero anche solo pochi anni fa alle minacce di attacchi informatici. Ciò nonostante, da più parti si rileva che (in Italia) le imprese allocano risorse ancora insufficienti alla sicurezza informatica e che, per altro verso, c'è penuria di forza lavoro adeguatamente formata.

È vero che il recepimento della Direttiva nel nostro ordinamento richiederà ancora del tempo: ma non c'è

dubbio che questo inevitabile intervallo, se doverosamente sfruttato, offre un'inaspettata opportunità sia alle imprese italiane che ai nostri giovani della generazione Z (e non solo).
Le prime, consapevoli dei più stringenti canoni di sicurezza informatica cui dovranno giocoforza conformarsi, potranno pianificare la propria strategia in materia di cybersecurity – colmando il gap fin qui creatosi rispetto, ad esempio, alle loro omologhe del Nord Europa – e dotarsi degli strumenti e delle risorse (professionali) necessarie ad attuarla; i secondi, consapevoli a loro volta che l'offerta di lavoro sarà sempre più orientata verso professionalità "digitali", potranno indirizzare opportunamente i loro studi e trovarsi pronti alla chiamata (che inevitabilmente nei prossimi anni sarà ancora più consistente di quanto non lo sia già oggi).

Avv. Gianmatteo Nunziante
Nunziante Magrone Studio Legale

Note:

[1] Relazione che accompagna la proposta di Direttiva NIS 2.

[2] Si tratta dei settori, in parte già individuati dalla vigente Direttiva NIS, dell'energia, dei trasporti, delle banche, dei mercati finanziari, della sanità, dell'acqua potabile, delle acque reflue, delle infrastrutture digitali, della gestione dei servizi ICT, degli enti della pubblica amministrazione e dello spazio.

[3] Si tratta dei settori dei servizi postali e di corriere, della gestione dei rifiuti, della fabbricazione, produzione e distribuzione di prodotti chimici, della produzione, trasformazione e distribuzione di alimenti, della fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro, della fabbricazione di computer e di prodotti di elettronica e ottica, della fabbricazione di apparecchiature elettriche, della fabbricazione di macchinari e apparecchiature n.c.a., della fabbricazione di veicoli a motore, rimorchi e semirimorchi, della fabbricazione di altri mezzi di trasporto e dei fornitori di servizi digitali.

[4] È questo il caso, ad esempio, di quelle imprese – quale che sia la loro dimensione – fornitrici uniche in un dato Stato Membro di un servizio essenziale per il mantenimento di attività sociali o economiche critiche; ovvero di quelle imprese che forniscano servizi la cui interruzione potrebbe avere un impatto significativo sulla sicurezza, l'incolumità o la salute pubblica; o ancora di quelle imprese la cui fornitura di servizi, se interrotta, potrebbe provocare un significativo rischio sistemico, specie se di dimensione transfrontaliera.

[5] La Direttiva elenca gli elementi che non possono mancare in tali misure: l'analisi dei rischi e politiche di sicurezza dei sistemi informatici, la gestione degli incidenti, la continuità operativa e gestione delle crisi, la sicurezza della catena di approvvigionamento, la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici di rete, le strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza, policy relativo all'uso della crittografia e della cifratura e sicurezza delle risorse umane.

[6] Un incidente è significativo se i) ha causato o può causare una perturbazione operativa o perdite finanziarie gravi per il soggetto interessato; ii) si è ripercosso o può ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

LE NOVITÀ DEL CODICE DELLA CRISI RELATIVE AGLI ASSETTI SOCIETARI ED IMPRENDITORIALI

Il Codice della Crisi non si è limitato a riformare le procedure concorsuali del nostro ordinamento ma ha anche previsto modifiche degli assetti delle imprese "in bonis" che incidono nell'organizzazione delle stesse, incluse quelle di dimensioni medio piccole.

La recente **riforma della disciplina del fallimento** (rectius: liquidazione giudiziale, secondo la nuova definizione adottata dal legislatore) si pone l'obiettivo di **anticipare la percezione dello stato di crisi della società** al fine di **intervenire tempestivamente e promuovere il risanamento dell'impresa**, evitando che la procedura concorsuale si limiti a vendere gli assets al miglior prezzo distribuendo il ricavato ai creditori.
Uno degli assi portanti del nuovo Codice della Crisi è rappresentato dall'**obbligo di ogni imprenditore** (incluse, quindi, le imprese individuali) di **dotarsi di adeguati assetti organizzativi, amministrativi e contabili** al fine di **rilevare tempestivamente** la crisi di impresa e la perdita della continuità aziendale.
La formula usata dal legislatore è ampia e, a prima vista, può sembrare una previsione generale, priva di riflessi pratici nell'organizzazione e nella gestione dell'attività di impresa. Invece essa comporta un **diverso approccio nel management delle società**, soprattutto quelle medio-piccole che hanno spesso basato l'attività sulle promettenti e profittevoli idee e iniziative del fondatore e degli amministratori in assenza di una programmazione di medio e lungo periodo e di una periodica misurazione delle performance aziendali.
In buona sostanza le imprese sono ora **tenute a porre in essere un sistema aziendale che consenta di controllare la presenza dell'equilibrio economico-**

finanziario e di monitorare il prevedibile andamento della gestione.
Qualora, a seguito di tali periodiche verifiche emerga l'insorgenza di uno stato di crisi, l'imprenditore dovrà avvalersi degli strumenti – anche di natura premiale – previsti dal Codice della Crisi per **evitare l'aggravamento della situazione**. Ciò comporta, inevitabilmente, un (apparente) aumento dei costi a carico dell'imprenditore, che dovrà coinvolgere consulenti aziendali e legali per dotarsi degli strumenti necessari per integrare il proprio assetto imprenditoriale. In realtà **tale spesa rappresenta un investimento** che mostrerà i propri vantaggi nel medio-lungo periodo, assicurando il perseguimento dell'equilibrio economico finanziario o, quanto meno, consentendo alla società/ impresa di avvalersi di un costante **monitoraggio delle performance registrate (o mancate)**, indirizzando le successive scelte di management in modo mirato e, auspicabilmente, più profittevole (o meno peggiorativo rispetto alla situazione in cui nessuno strumento di misurazione e verifica dei risultati sia posto in essere).

Ovviamente **non esiste un modello di assetto adeguato generale e replicabile in tutti i casi**, dato che esso dipende dal settore di attività e dalle dimensioni dell'impresa. Ad esempio, nei casi più semplici potrà essere sufficiente impostare, con l'ausilio del consulente di fiducia, il **calcolo di indici di redditività e sostenibilità economica** utilizzando dati già a disposizione degli amministratori e verificare con essi gli impatti degli investimenti programmati.

Avv. Patrizio Cataldo
Cocuzza & Associati, Studio Legale

PRIVACY

GARE DI APPALTO E PRIVACY: IL TEMA DEL DIRITTO DI ACCESSO

Talvolta la disciplina di accesso agli atti si interseca con la disciplina in materia di protezione dei dati personali (privacy).
Ciò accade ogni volta che i documenti oggetto della richiesta di accesso contengono dati personali, siano essi comuni o appartenenti alle categorie particolari di cui all'art. 9 GDPR o all'art. 10 GDPR.

In tema di appalti si parla, ad esempio, della domanda di partecipazione, che contiene sicuramente dati personali del partecipante, come i dati anagrafici del legale rappresentante della società. Si parla anche dei curriculum vitae del personale coinvolto nelle attività, o la documentazione che dimostra il possesso dei titoli, competenze ed esperienze. Ancora, si può parlare di elementi riservati contenuti nell'offerta tecnica di gara e inerenti al know how aziendale. Quest'ultimo specificamente tutelato in materia d'accesso dall'art. 53 co. 5 lett. a) D.lgs. 50/2016.
Tutti i documenti citati (così come anche altri) contengono o possono contenere dati personali.
Ciò comporta che, a fronte di un'istanza di accesso, l'amministrazione debba sempre tenere in conto che l'ostensione di determinati documenti potrebbe comportare la diffusione anche dei dati personali che tali documenti contengono.

Ci si chiede, quindi, se tali documenti possano essere oggetto di istanza di accesso e in che modo debbano essere tenuti in considerazione i diritti che la disciplina in materia di protezione dei dati personali riconosce in capo ad ogni soggetto.
La risposta si trova, da un lato, in una valutazione basata sul bilanciamento tra gli **obblighi di trasparenza** e gli **obblighi di protezione dei dati** cui è soggetta l'amministrazione – o, meglio, nell'individuazione e nella valutazione di un eventuale pregiudizio agli interessati a cui i dati si riferiscono nel caso in cui tali dati venissero conosciuti da terzi – dall'altro nella tipologia di diritto all'accesso che è stato esercitato, se ai sensi della l.n. 241/1990 c.d. accesso documentale o se ai sensi del D.lgs. 33/2013 c.d. accesso civico.

Il tema è stato affrontato più volte dal Garante per la protezione dei dati personali che, pur riconoscendo la rilevanza del diritto di accesso nell'ambito di procedure di appalto, ha riconosciuto un ruolo prevalente ai diritti di riservatezza degli interessati.
In una di queste occasioni il Garante si è espresso su una istanza di accesso civico che aveva ad oggetto un'importante mole di dati personali.
Nell'ambito di un appalto di servizi, l'istante aveva infatti richiesto di ottenere dati, informazioni e documenti contenenti un gran numero di dati personali (riferiti a più di 1.700 soggetti) riguardanti, in particolare, la lista del personale utilizzato nei vari servizi, il curriculum vitae del personale, la

documentazione comprovante il possesso dei titoli e le competenze di ciascun soggetto.
Ci si è chiesti se l'ostensione di tali dati fosse pregiudizievole al diritto alla riservatezza, posto che per valutare la correttezza della procedura di gara e delle successive fasi prodromiche all'aggiudicazione fosse necessario esaminare proprio quella documentazione.
Nonostante nel caso di specie fosse esclusa la possibilità di proporre istanza di accesso civico generalizzato, il Garante ha colto l'occasione per evidenziare come, in linea generale, debba essere tenuta in considerazione la circostanza per la quale (a differenza dei documenti a cui si è avuto accesso ai sensi della l. n. 241 del 7/8/1990) i dati e i documenti che si ricevono a seguito di una istanza di accesso civico divengono "pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7", sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 3, comma 1, del d. lgs. N. 33/2013).

Di conseguenza, precisa il Garante, "*è anche alla luce di tale amplificato regime di pubblicità dell'accesso civico che va verificata l'esistenza di un possibile pregiudizio concreto alla protezione dei dati personali dei soggetti controinteressati, in base al quale decidere se rifiutare o meno l'accesso civico alle informazioni e ai documenti richiesti*".
Pertanto, "*la decisione sulla eventuale ostensione di dati personali nell'ambito del procedimento di accesso civico, deve inoltre tener conto anche nel rispetto dei principi indicati dall'art. 5 del Regolamento (UE) 2016/679 (RGPD), fra cui quello di «minimizzazione dei dati», secondo il quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 5, par. 1, lett. c), in modo che non si realizzi un'interferenza ingiustificata e sproporzionata nei diritti e libertà delle persone cui si riferiscono tali dati*".

Nel caso di specie i documenti richiesti con l'accesso civico sono tutti afferenti alla rivelazione di informazioni su attitudini, capacità culturali, professionali e lavorative dei soggetti controinteressati e per questo il Garante ha evidenziato come la relativa ostensione, "*considerata anche la quantità e qualità dei dati personali coinvolti, può avere – in relazione ai casi e al contesto in cui possono essere utilizzate da parte di terzi estranei che non è dato conoscere a priori – possibili ripercussioni negative sul piano relazionale, personale, sociale dei soggetti controinteressati, sia all'interno che all'esterno dell'ambiente lavorativo*".

In definitiva, permettere l'ostensione di ogni dato costituirebbe un'interferenza ingiustificata e sproporzionata rispetto ai diritti ed alle libertà dei soggetti controinteressati, in violazione del GDPR e dei suoi principi.

Avv. Eleonora Pettazzoni e Avv. Maddalena Collini
Studio Legale Stefanelli

L'OGGETTO DELLA GARA DI APPALTO RACCOGLIE TROPPI DATI? AGGIUDICAZIONE ANNULLATA DAL TAR

TAR Veneto, Sez. I, 4/01/2022, nr. 8

Il provvedimento riguarda un autovelox, ma l'azienda produttrice di qualsiasi dispositivo che tratta dati personali potrebbe conoscere la stessa sorte della società che si è vista annullare il provvedimento di aggiudicazione di una gara di appalto per non aver rispettato uno dei principi fondamentali del Regolamento privacy (GDPR): la minimizzazione dei dati.

Minimizzare i dati significa utilizzare solo quelli indispensabili rispetto alla finalità legittima che si vuole raggiungere: obbligo, questo, previsto dall'art. 5 del GDPR e applicabile in via generale a tutti i trattamenti di dati.

Effettivamente, il dispositivo per la rilevazione delle infrazioni oggetto della gara non risultava conforme alle specifiche stabilite dalla stazione appaltante: il capitolato riportava, infatti, "i beni oggetto dell'appalto dovranno essere conformi e rispondenti, per caratteristiche, prescrizioni omologazioni e approvazioni, alle norme contenute nel Codice della Strada, nel relativo Regolamento di Esecuzione e ad **ogni altra normativa e disciplina che regolamenti la materia**".
Innegabile che le postazioni omologate per il servizio di controllo elettronico della velocità effettuino un trattamento dei dati personali dei conducenti dei veicoli che va a ricadere nell'ambito di applicazione della normativa privacy: di conseguenza anche il trattamento

dei loro dati deve essere minimizzato, e quindi limitato allo stretto necessario.

Ma in che senso l'aggiudicataria non aveva minimizzato i dati?
La procedura di gara riguardava l'affidamento del servizio di noleggio, installazione e manutenzione di dispositivi per il controllo elettronico di infrazioni stradali.
Con il primo motivo la ricorrente rilevava che l'aggiudicataria aveva proposto il noleggio di un dispositivo che, oltre a rilevare le infrazioni al codice della strada ("*controllo delle infrazioni al semaforo rosso*" e "*accertamento della velocità*"), **registra in modo generico e indifferenziato tutti i veicoli che transitano nel raggio di azione del dispositivo, verificando in automatico tramite banche dati, ovvero senza l'interposizione di un operatore, anche il rispetto di obblighi di revisione e di assicurazione**.

Il TAR Lazio sottolinea che i dispositivi di controllo utilizzati per l'accertamento delle infrazioni al codice della strada non possono registrare i dati di tutti i veicoli in transito ma solo di quelli che commettono l'infrazione; a sostegno il TAR richiama il Consiglio di Stato, che con la sentenza n. 509 del 2021 richiama importanti principi in tema di trattamento dei dati ovvero

- il controllo di tipo indiscriminato è vietato
- le immagini sono memorizzate solo in caso di infrazione e sono utilizzabili solo per l'accertamento e la contestazione degli illeciti stradali
- la registrazione continua dei dati del traffico è conservata in forma di dati anonimi e i dati possono essere utilizzati solo per studi o ricerche sul traffico
- le immagini sono trattate solo dagli incaricati del trattamento previamente individuati
- le immagini sono conservate solo per il periodo strettamente necessario.

In definitiva, l'**aggiudicazione dell'appalto avrebbe comportato una raccolta sproporzionata di dati**: per questo motivo è stata annullata.
Se da questo provvedimento si deve trarre un insegnamento è senza dubbio quello per cui le conseguenze del mancato rispetto della disciplina sulla protezione dei dati non sono soltanto le – seppur molto temute per gli importi che possono raggiungere – sanzioni amministrative pecuniarie (art. 83 GDPR).

La conformità al GDPR e al Codice Privacy, oltre che ai numerosi provvedimenti e linee guida emanati dall'Autorità Garante e dalle istituzioni comunitarie, **è diventata un vero e proprio criterio di valutazione delle offerte per l'aggiudicazione degli appalti**.

La giurisprudenza si sta orientando sempre di più in questo senso, creando una **nuova consapevolezza in chi partecipa alle gare sia private che pubbliche**.
È una consapevolezza che si va necessariamente a sostituire all'ormai abbandonato preconcetto che vuole la "privacy" intesa solo come tutela della sfera privata degli individui e come formalismo che può essere soddisfatto consegnando un'informativa e richiedendo un consenso (spesso nemmeno dovuto) per poi essere accantonato.

La protezione dei dati è invece una materia viva, che nelle procedure di gara – come in molti altri contesti nei rapporti di fornitura – può fare la differenza. E che nel caso sottoposto al TAR Veneto, l'ha concretamente fatta a scapito dell'aggiudicataria.

Avv. Eleonora Lenzi e Avv. Maria Livia Rizzo
Studio Legale Stefanelli

SERVIZI ONLINE, NECESSARIO L'UTILIZZO DI PROTOCOLLI SICURI: MULTA DI 15 MILA EURO AD UN'AZIENDA CHE UTILIZZAVA UN PROTOCOLLO DI COMUNICAZIONE IN CHIARO

Per scongiurare il rischio di furti d'identità e garantire una adeguata tutela dei dati personali, l'interazione degli utenti con un sito web ai fini della trasmissione di dati personali deve essere protetta con protocolli crittografici (come quello "https").
È quanto ha ribadito il Garante privacy sanzionando un'Azienda fornitrice di servizi idrici per 15.000 euro, per non aver protetto adeguatamente i dati dei clienti registrati sull'area riservata del proprio sito web.
A seguito di un reclamo l'Autorità ha accertato che l'accesso al sito web dell'Azienda dedicato ai "servizi online" avveniva tramite il protocollo di rete "http", non crittografato e non sicuro.
Diversi i dati personali dei clienti che transitavano mediante tale canale, dalle credenziali di autenticazione (nome utente e password) alle anagrafiche, con nomi, cognomi, codici fiscali/partite IVA, indirizzi di posta elettronica, numeri di telefono e dati di fatturazione. La soluzione adottata dall'Azienda violava importanti

principi sanciti dal Regolamento come quello di "integrità e riservatezza" dei dati trattati, in base al quale il titolare deve mettere in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, come la cifratura dei dati personali, e quello di "protezione dei dati fin dalla progettazione", secondo il quale occorre mettere in atto, fin dall'inizio, misure tecniche e organizzative adeguate a tutelare i dati personali e successivamente effettuare revisioni periodiche delle misure di sicurezza adottate.
Tali obblighi, ha precisato il Garante, si applicano anche ai sistemi preesistenti alla data di efficacia del Regolamento (25 maggio 2018).
Nel sanzionare l'Azienda per 15.000 euro l'Autorità ha tenuto conto dell'alto numero di utenti coinvolti (circa 13.000) e del fatto che, sebbene il reclamante avesse fatto presente all'Azienda in due occasioni l'insufficienza delle misure di sicurezza adottate, questa non si era prontamente attivata fino all'apertura dell'istruttoria.
Di contro, il Garante ha tenuto in considerazione che l'Azienda non aveva commesso precedenti violazioni analoghe e aveva avuto un atteggiamento collaborativo nel corso dell'istruttoria.

Fonte: https://www.garanteprivacy.it/home

RINNOVABILI

EOLICO: ILLECITO IL DINIEGO ALLA REALIZZAZIONE DI UN IMPIANTO EOLICO SE NON MOTIVATO IN CONCRETO

Consiglio di Stato, sez. IV, sentenza n. 10664 del 6.12.2022

Nella sentenza in oggetto il CdS ha esaminato l'appello presentato da una società operante nel settore degli impianti eolici, contro la sentenza con cui il TAR della Basilicata aveva rigettato il ricorso con cui la medesima società aveva impugnato il parere sfavorevole di compatibilità ambientale dato dalla Regione Basilicata in merito alla realizzazione da parte della società di un mini impianto eolico nel comune di Potenza.

In particolare, il parere sfavorevole si basava sui seguenti rilievi:

- il nuovo impianto, sommandosi ad altri impianti già installati, avrebbe contribuito ad un maggiore impatto visivo d'assieme (effetto cosiddetto "selva");
- l'altezza dell'impianto sarebbe stata fuori scala rispetto agli impianti già presenti;
- la turbina sarebbe stata percepibile da due siti di interesse archeologico, pur non ricadendo in area vincolata.

Il Consiglio di Stato, però, ha accolto l'appello presentato dall'operatore, indicando che <l*'aggravamento dell'effetto 'selva' andava motivato in concreto, tenuto conto che si tratta di un solo aerogeneratore che si inserisce in un contesto che vede non solo la presenza di 20 impianti (13 già realizzati e 7 autorizzati) ma anche di altri parchi eolici limitrofi e prossimi alle zone archeologiche (…) sicché il valore marginale in termini di potenziale pregiudizio paesaggistico è oggettivamente ridotto e, come tale, andava puntualmente giustificato in relazione alle caratteristiche dei luoghi*>.

Secondo il CdS poi <*non appare dirimente il dato della altezza dell'impianto – ritenuta sproporzionata rispetto al mini eolico presente nell'area – poiché tale criticità […] era comunque superabile, tenuto conto della disponibilità manifestata dalla appellante, in sede di controdeduzioni al preavviso di diniego, a ridurre le dimensioni dell'impianto*>.

Il Consiglio quindi, in riforma della sentenza del TAR appellata, ha accolto il ricorso di primo grado e annullato i provvedimenti di diniego impugnati.

SICUREZZA PRODOTTI ED IMPIANTI

BREXIT: SLITTAMENTO OBBLIGO MARCATURA UKCA ANCHE PER CPR

A completamento della notizia già data sul numero di novembre/dicembre 2022 del Telex ANIE, circa l'ulteriore proroga dell'obbligo di marcatura UKCA, si segnala che per prodotti soggetti alla normativa sui prodotti da costruzione (per la UE , il reg. 305/2011 cosiddetto CPR) la proroga è al **30 giugno 2025**.
Fino ad allora i prodotti potranno essere venduti in UK con la sola marcatura CE.

Fonte:
https://www.gov.uk/guidance/construction-products-regulation-in-great-britain

IMPIANTI ELETTRONICI: MODIFICHE AL DM 37/2008

E' stato pubblicato sulla GURI n. 290 del 13 dicembre 2022 il **DM 192 del 29 settembre 2022** che introduce alcune modifiche al DM 37/2008 in materia di sicurezza degli impianti al servizio degli edifici.
In particolare, le modifiche riguardano gli impianti elettronici di cui all'art. 1, comma 2 lett. b) del DM 37 individuati ora in modo più puntuale come < *impianti radiotelevisivi, le antenne, gli impianti elettronici deputati alla gestione e distribuzione dei segnali tv, telefono e dati, anche relativi agli impianti di sicurezza compresi gli impianti in fibra ottica, nonché le infrastrutture necessarie ad ospitare tali impianti*> [i].

Conseguentemente, è modificata anche la definizione di impianti radiotelevisivi ed elettronici di cui all'art. 2 lett. f) del DM 37/08 che, per effetto delle modifiche, fa adesso riferimento a <*le componenti impiantistiche necessarie alla trasmissione ed alla ricezione dei segnali tv, telefono e dati, anche relativi agli impianti di sicurezza, ad installazione fissa, comprese le infrastrutture destinate ad ospitare tali impianti*>[ii].
Viene integrata anche la definizione di punto di consegna di cui all'articolo 2, comma 1, lettera a) del DM 37, con l'aggiunta alla fine delle seguenti parole <*ovvero il punto terminale di rete come definito dall'articolo 2, comma 1, lettera oo), del decreto legislativo 8 novembre 2021, n. 207*>[iii].

Per gli impianti così ridefiniti di cui all'art. 1, comma 2 lett. b) del DM 37, il nuovo DM prevede che il responsabile tecnico dell'impresa sia responsabile dell'inserimento nel progetto edilizio dell'edificio di tutte le parti di infrastruttura fisica multiservizio passiva e degli accessi che richiedono di essere realizzati per gli interventi per l'infrastrutturazione digitale degli edifici previsti dall'articolo 135-bis [iv] del DPR 380/2001 TU EDILIZIA.
Al termine dei lavori, su istanza del soggetto che ha richiesto il rilascio del permesso di costruire o di altro soggetto interessato, il responsabile tecnico dell'impresa rilascia una dichiarazione di conformità dell'impianto ai sensi di quanto previsto dalle Guide CEI 306-2, CEI 306-22 e 64-100/1, 2 e 3, corredata degli allegati ove sono descritte le caratteristiche degli accessi e della infrastruttura fisica multiservizi passiva. Tale dichiarazione è necessaria ai fini della presentazione allo sportello unico dell'edilizia della segnalazione certificata di cui all'articolo 24 del DPR 380/2001.

Le nuove norme saranno in vigore dal 28 Dicembre 2022.

Note:

[i] La vecchia dizione è <*impianti radiotelevisivi, le antenne e gli impianti elettronici in genere*>.

[ii] Il vecchio testo della norma definisce gli impianti radiotelevisivi ed elettronici come <*le componenti impiantistiche necessarie alla trasmissione ed alla ricezione dei segnali e dei dati, anche relativi agli impianti di sicurezza, ad installazione fissa alimentati a tensione inferiore a 50 V in corrente alternata e 120 V in corrente continua, mentre le componenti alimentate a tensione superiore, nonché i sistemi di protezione contro le sovratensioni sono da ritenersi appartenenti all'impianto elettrico; ai fini dell'autorizzazione, dell'installazione e degli ampliamenti degli impianti telefonici e di telecomunicazione interni collegati alla rete pubblica, si applica la normativa specifica vigente*>

[iii] In realtà la definizione è prevista dall'art. 2, comma 1 lett. oo) del DLGS 257 del 2003 come modificato con DLGS 207 del 2021: <*punto terminale di rete: il punto fisico a partire dal quale l'utente finale ha accesso a una rete pubblica di comunicazione elettronica e che, in caso di reti in cui abbiano luogo la commutazione o l'instradamento, è definito mediante un indirizzo di rete specifico correlabile a un numero di utente finale o a un nome di utente finale; per il servizio di comunicazioni mobili e personali il punto terminale di rete è costituito dall'antenna fissa cui possono collegarsi via radio le apparecchiature terminali utilizzate dagli utenti del servizio*>.

[iv] Si riporta il testo dell'art. 135-bis *Norme per l'infrastrutturazione digitale degli edifici* del TU Edilizia:
<*1. Tutti gli edifici di nuova costruzione per i quali le domande di autorizzazione edilizia sono presentate dopo il 1° luglio 2015 devono essere equipaggiati con un'infrastruttura fisica multiservizio passiva interna all'edificio, costituita da adeguati spazi installativi e da impianti di comunicazione ad alta velocità in fibra ottica fino ai punti terminali di rete. Lo stesso obbligo si applica, a decorrere dal 1° luglio 2015, in caso di opere che richiedano il rilascio di un permesso di costruire ai sensi dell'articolo 10, comma 1, lettera c). Per infrastruttura fisica multiservizio interna all'edificio si intende il complesso delle installazioni presenti all'interno degli edifici contenenti reti di accesso cablate in fibra ottica con terminazione fissa o senza fili che permettono di fornire l'accesso ai servizi a banda ultralarga e di*

connettere il punto di accesso dell'edificio con il punto terminale di rete.

2. *Tutti gli edifici di nuova costruzione per i quali le domande di autorizzazione edilizia sono presentate dopo il 1° luglio 2015 devono essere equipaggiati di un punto di accesso. Lo stesso obbligo si applica, a decorrere dal 1° luglio 2015, in caso di opere di ristrutturazione profonda che richiedano il rilascio di un permesso di costruire ai sensi dell'articolo 10. Per punto di accesso si intende il punto fisico, situato all'interno o all'esterno dell'edificio e accessibile alle imprese autorizzate a fornire reti pubbliche di comunicazione, che consente la connessione con l'infrastruttura interna all'edificio predisposta per i servizi di accesso in fibra ottica a banda ultralarga.*

*2-bis. Per i nuovi edifici nonché in caso di nuove opere che richiedono il rilascio di permesso di costruire ai sensi dei commi 1 e 2, per i quali la domanda di autorizzazione edilizia sia stata presentata dopo la data del 1° gennaio 2022, l'adempimento dei prescritti obblighi di equipaggiamento digitale degli edifici è attestato dall'etichetta necessaria di "edificio predisposto alla banda ultra larga", rilasciata da un tecnico abilitato per gli impianti di cui all'*articolo 1, comma 2, lettera b), del decreto del Ministro dello sviluppo economico 22 gennaio 2008, n. 37, *e secondo quanto previsto dalle Guide CEI 306-2, CEI 306-22 e 64-100/1, 2 e 3, su istanza del soggetto che ha richiesto il rilascio del permesso di costruire o di altro soggetto interessato. Tale attestazione è necessaria ai fini della segnalazione certificata di cui all'articolo 4. Il Comune entro 90 giorni dalla ricezione della segnalazione è tenuto a comunicare i dati relativi agli edifici infrastrutturali al Sistema Informativo Nazionale Federato delle Infrastrutture (SINFI) ai sensi del* decreto-legge 12 settembre 2014, n. 133 convertito con modificazioni dalla legge n. 164 del 2014.

3. *Gli edifici equipaggiati in conformità al presente articolo, per i quali la domanda di autorizzazione edilizia sia stata presentata prima del 1° gennaio 2022, possono beneficiare ai fini della cessione, dell'affitto o della vendita dell'immobile, dell'etichetta volontaria e non vincolante di 'edificio predisposto alla banda ultra larga', rilasciata da un tecnico abilitato come previsto dal comma 2-bis. >.*

DIRETTORE RESPONSABILE
Maria Antonietta Portaluri

REDAZIONE
Alessandra Toncelli – Mirella Cignoni

LA REDAZIONE RINGRAZIA PER LA COLLABORAZIONE

Avv. Silvia Bortolotti, BBM Partners, Buffa, Bortolotti & Mathis (Torino – www.bbmpartners.com) - Avv. Luca Feltrin, Freshfields Bruckhaus Deringer (Milano – www.freshfields.com) - Avv. Patrizio Cataldo, Cocuzza & Associati, Studio Legale (Milano – www.cocuzzaeassociati.it) - Avv. Gianmatteo Nunziante, Nunziante Magrone Studio Legale (Roma, Milano, Bologna – www.nunziantemagrone.it) - Avv. Maddalena Collini, Avv. Eleonora Lenzi, Avv. Eleonora Pettazzoni e Avv. Maria Livia Rizzo, Studio Legale Stefanelli (Bologna – www.studiolegalestefanelli.it)

Proprietario ed editore:
Federazione ANIE
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.1
Direttore Responsabile
Maria Antonietta Portaluri
Registrazione del Tribunale
di Milano al n° 116 del
19/2/1996

TeLex Anie

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE
CONFINDUSTRIA

Pubblicazione a cura di:
Servizio Centrale Legale
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.246
e-mail legale@anie.it
Diffusione via web www.anie.it

Approfondimento del mese di Gennaio 2023

ADEGUAMENTO DEI CONTRATTI E DELLE RETI DISTRIBUTIVE AL NUOVO REGOLAMENTO SULLA CONCORRENZA (REG. UE 720/2022)

Com'è noto, il 10 maggio 2022 è stato adottato il nuovo Regolamento UE di esenzione per categoria degli accordi verticali (Regolamento 720/2022, anche denominato "VBER") e le relative Linee Guida.

Il Regolamento è entrato in vigore il 1° giugno 2022. Tuttavia, le nuove disposizioni si applicheranno ai contratti già in vigore al 31 maggio 2022 - e conformi al precedente Reg. 330/2010 - solo a partire dal 31 maggio 2023: entro tale termine dovranno quindi essere apportate le eventuali modifiche ai contratti di distribuzione (esclusiva e/o selettiva) e di franchising, necessarie per renderli conformi alle nuove norme e, alla luce delle novità introdotte, questa potrà essere l'occasione per studiare e valutare nuove strategie di riorganizzazione della propria rete distributiva offline e online.

Risulta quindi importante accennare alle principali novità introdotte dal nuovo Regolamento e dalle Linee Guida.

1. Le restrizioni alle vendite online nei contratti di distribuzione e franchising

Una delle modifiche più importanti consiste nell'introduzione nel Regolamento di una chiara definizione delle nozioni di "vendite attive" e "vendite passive" (articolo 1, paragrafo 1, lettere (l) e (m)).
In precedenza, tali definizioni erano incluse solo nelle Linee Guida (§ 51) e, rispetto al nuovo testo, erano previste una nozione più ampia di "vendite passive" e una più restrittiva di "vendite attive"; ma anche le relative definizioni erano poco chiare e lasciavano spazio ad un elevato livello di incertezza.
Risultava pertanto difficile per le imprese valutare la conformità di eventuali restrizioni imposte ai propri distributori/franchisee, in particolare per quanto riguardava le vendite e le promozioni via internet, a fronte di un elevato rischio che le stesse potessero essere considerate vietate. È quindi molto apprezzabile la chiarezza delle nuove definizioni, la loro inclusione nel Regolamento (anziché solo nelle Linee Guida) ed il fatto che vi sia ora una nozione più ampia di "vendite attive" e una più restrittiva di "vendite passive", che risultano più rispondenti alle modalità di promozione e vendita online oggi effettivamente utilizzate.

Ma la modifica più importante a questo riguardo, consiste nell'introduzione di una nuova e specifica restrizione fondamentale, relativa all'uso di internet (art. 4, paragrafo 1, lettera e)), individuata nei termini seguenti:

«e) la pratica di impedire l'uso efficace di internet da parte dell'acquirente o dei suoi clienti per vendere i beni o servizi oggetto del contratto, in quanto tale pratica limita il territorio in cui, o i clienti ai quali, i beni o servizi oggetto del contratto possono essere venduti ai sensi delle lettere b), c) o d), fatta salva la possibilità di imporre all'acquirente:

   i) altre restrizioni delle vendite online; o
   ii) restrizioni della pubblicità online che non hanno lo scopo di impedire l'uso di un intero canale pubblicitario online;»

Ciò significa che un divieto generale, diretto o indiretto, dell'uso di internet è certamente vietato; tuttavia, sono ammesse restrizioni alla vendita e alla pubblicità online, nella misura in cui esse non impediscano l'uso efficace di internet.

A questo proposito, le nuove Linee Guida (anche recependo i principi elaborati dalla giurisprudenza comunitaria) forniscono esempi ed indicazioni specifiche circa le restrizioni che possono (cfr. §§ 208-210) e non possono (cfr. § 206) essere imposte. Ad esempio:

- non è possibile imporre all'acquirente di vendere i beni o i servizi oggetto del contratto solo in uno spazio fisico o alla presenza fisica di personale specializzato (cfr. Linee Guida, § 206 (c));
- al contrario, è consentito prevedere un divieto diretto o indiretto di utilizzo di *marketplaces* online (cfr. Linee Guida, § 208 (c));
- è possibile richiedere che l'acquirente paghi un prezzo all'ingrosso diverso per i prodotti venduti online rispetto a quelli venduti offline, se giustificato, ad esempio, da costi e investimenti (c.d. *dual pricing* - cfr. Linee Guida, § 209);
- è possibile prevedere un obbligo di vendere una quantità minima di beni o servizi offline, sulla base di criteri oggettivi (cfr. Linee Guida, § 208 (e), ipotesi che peraltro era già prevista nelle precedenti Linee Guida).

Per quanto riguarda la pubblicità online, l'articolo 4 (e) del Regolamento prevede che non si possa limitare un "intero canale pubblicitario online" e le Linee Guida citano, come possibili esempi, i motori di ricerca o i servizi di comparazione dei prezzi. Tuttavia, anche a questo riguardo le Linee Guida offrono alcune indicazioni utili per trovare soluzioni contrattuali adeguate, che devono essere considerate anche alla luce della giurisprudenza comunitaria precedente, ad esempio in materia di AdWords.

In conclusione, per quanto riguarda le vendite e la pubblicità online, le aziende dovranno quindi astenersi dall'imporre restrizioni che abbiano come obiettivo diretto o indiretto quello di impedire l'uso effettivo di internet da parte del distributore/franchisee; entro questo limite, potranno essere imposte al distributore eventuali restrizioni alle vendite online, ma occorrerà anche verificare che tali restrizioni rimangano coerenti con lo specifico sistema di distribuzione utilizzato (ad es. rete esclusiva o rete selettiva). In ogni caso, occorre poi sempre considerare i possibili effetti cumulativi delle diverse restrizioni.

2. Restrizioni territoriali: possibile riorganizzazione della rete distributiva

Per quanto riguarda le restrizioni territoriali, il precedente Regolamento prevedeva un divieto generale di restrizioni territoriali e, come eccezione, consentiva solo
(i) la restrizione delle vendite attive a territori o gruppi di clienti assegnati in esclusiva ad altri distributori (o riservati al fornitore);
(ii) la restrizione delle vendite agli utenti finali da parte di acquirenti che operano a livello di commercio all'ingrosso; e
(iii) la restrizione delle vendite attive e passive da parte dei membri di un sistema di distribuzione selettiva a distributori non autorizzati all'interno del territorio riservato dal fornitore per la gestione di tale sistema (si veda l'articolo 4, lettera b), punti i), ii) e iii) del Reg. 330/2010).

Ora, l'articolo 4, lettere (b), (c) e (d) del nuovo Regolamento fornisce una descrizione dettagliata delle restrizioni territoriali e alla clientela ammissibili e vietate, distinguendo tra
(i) distribuzione esclusiva;
(ii) distribuzione selettiva; e
(iii) distribuzione libera (cioè distribuzione non esclusiva e non selettiva), fornendo una maggiore chiarezza sulle interazioni tra i diversi canali distributivi.

Per quanto riguarda le reti di distribuzione selettiva, esse ora possono essere protette dalle vendite attive e passive a distributori non autorizzati della rete, non solo da parte dei membri della stessa rete selettiva, ma anche da parte di distributori esterni alla rete. Ma il principio generale più innovativo in questo ambito è che il fornitore può ora richiedere ai suoi distributori di "trasferire" le stesse restrizioni anche ai loro clienti diretti (e, quando la restrizione protegge un sistema selettivo, anche più in basso nella catena di distribuzione). Si tratta di una modifica molto importante, che può garantire un livello di protezione più elevato nelle reti di distribuzione.
Tuttavia, traslare tali principi dalla teoria agli accordi effettivi, garantendo un coerente coordinamento tra le varie reti di vendita nei diversi territori dell'Unione Europea non è così facile e permangono purtroppo varie criticità, che erano state segnalate alla Commissione UE in fase di revisione.

Per quanto riguarda gli accordi di franchising, in linea di principio essi possono rientrare nell'ambito di applicazione delle norme di ciascun sistema, a seconda del modello di distribuzione scelto dall'affiliante, ad esempio selettivo o esclusivo (cfr. § 167 delle Linee Guida). In pratica, nella maggior parte dei casi non vi è una scelta esplicita né a favore del sistema selettivo (ad esempio introducendo nel contratto di franchising disposizioni esplicite in conformità all'articolo 4 (c) del Regolamento), né a favore del modello esclusivo (ad esempio prevedendo una restrizione alle vendite attive nei territori eventualmente attribuiti in esclusiva a ciascun affiliato). Tuttavia, è importante che la scelta di uno specifico sistema di distribuzione sia consapevole e coerente con le restrizioni previste dai relativi accordi.

3. "Dual distribution"

Una delle disposizioni più critiche introdotte nel nuovo Regolamento riguarda la c.d. duplice distribuzione ("dual distribution"). La questione si pone, ad esempio, quando le aziende vendono i loro prodotti online parallelamente alla rete di distribuzione fisica tradizionale, o quando i franchisor hanno negozi diretti sul territorio, in concorrenza con i negozi dei loro affiliati. Questa situazione porta il concedente/franchisor a competere con i membri della sua rete, il che può dare origine ad una restrizione orizzontale della concorrenza tra loro.
L'articolo 2 (4) del Reg. 330/2010 esentava gli accordi verticali non reciproci tra il fornitore e i suoi distributori in ragione del fatto che le due parti sono tipicamente concorrenti a valle, ma non a monte e quindi non dovrebbero sorgere particolari problemi di concorrenza.

Il nuovo VBER, oltre a riformulare gli artt. 2 (4) lettere a) e b), ha introdotto una disposizione aggiuntiva che esclude il beneficio dell'esenzione in caso di scambio di informazioni tra le due parti, tranne nel caso in cui tale scambio di informazioni sia
(i) direttamente connesso all'attuazione dell'accordo verticale; o
(ii) necessario per migliorare la produzione o la distribuzione dei beni o servizi oggetto del contratto. Le Linee Guida forniscono un elenco di esempi di possibili scambi di informazioni che probabilmente (§ 99) o difficilmente (§ 100) soddisfano le condizioni di cui sopra.

Le nuove norme impongono quindi una verifica caso per caso del tipo di informazioni scambiate e un difficile compito nella gestione di questi aspetti (considerando, ad esempio, i software e i database normalmente utilizzati nelle reti di franchising e distribuzione), che implica un irragionevole aumento dei costi per le imprese.
Per quanto riguarda le conseguenze di un'eventuale violazione della norma, ai sensi dei §§ 102-103 delle Linee Guida, nel caso in cui lo scambio di informazioni non soddisfi le due condizioni, lo scambio di informazioni dovrà essere valutato individualmente ai sensi dell'articolo 101 del Trattato; in ogni caso, le altre disposizioni dell'accordo verticale beneficeranno comunque dell'esenzione. Inoltre, si dovrà considerare la possibile applicazione della Comunicazione "De Minimis" con riguardo agli accordi che hanno un impatto non rilevante sul mercato.

4. Fornitori di servizi di intermediazione online (piattaforme online)

L'art. 1, par. 1, lett. e) del Reg. 720/2022 definisce i "servizi di intermediazione online" facendo riferimento alla nozione di "servizi della società dell'informazione" di cui alla Direttiva UE 2015/1535.
Tale nozione ha un ambito di applicazione molto ampio, in quanto può essere applicata ai *marketplaces*, agli *app stores,* piattaforme di consegna, ecc. Tale nozione si applica non solo quando la transazione viene conclusa sulla piattaforma, ma anche quando la piattaforma reindirizza i clienti verso altri siti web per la conclusione della transazione (cfr. § 332 delle Linee Guida): pertanto, vengono inclusi anche, ad esempio, strumenti di comparazione prezzi, servizi di social media, ecc. Può anche includere altre situazioni, ad esempio la piattaforma di un franchisor attraverso la quale sia il franchisor che i suoi affiliati possono vendere online ai clienti finali.
La definizione di "fornitore di servizi di intermediazione online" e la relativa disciplina si applica solo al caso in cui la piattaforma agisca come intermediario in una transazione conclusa tra l'impresa venditrice (che acquista i servizi di intermediazione) e il terzo acquirente/cliente. Al contrario, essa non si applica al caso in cui la piattaforma agisca come acquirente/rivenditore dei beni o servizi in questione.

Tuttavia, se la piattaforma ha una funzione ibrida (cioè agisce anche come acquirente/rivenditore degli stessi prodotti o servizi attraverso la piattaforma) l'accordo verticale non sarà esentato, né si applicherà l'esenzione prevista dall'art. 2, paragrafo 4, del VBER sullo scambio di informazioni nella "dual distribution".

Il rischio di perdere l'esenzione è certamente preoccupante per le imprese che agiscono come piattaforme ibride. Ad esempio, se consideriamo una piattaforma attraverso la quale un franchisor venda i propri prodotti e - allo stesso tempo - consenta e faciliti le vendite tra i propri franchisee e gli utenti finali dei medesimi prodotti, il franchisor avrà una funzione ibrida e, in linea di principio, non beneficerà dell'esenzione per categoria, né delle esenzioni sulla "dual distribution" (artt. 2 (6) e 2 (4) del VBER), con le conseguenze menzionate al precedente paragrafo.

Tuttavia, il § 109 delle Linee Guida specifica che:
«In assenza di restrizioni per oggetto o di un potere di mercato significativo, è improbabile che la Commissione attribuisca la priorità alle azioni di applicazione della normativa nei confronti di accordi verticali relativi alla fornitura di servizi di intermediazione online in cui il fornitore svolge una funzione ibrida. Questo vale in particolare quando, in uno scenario di duplice distribuzione, un fornitore consente agli acquirenti dei suoi beni o servizi di utilizzare il suo sito web per la distribuzione dei beni o servizi, ma non consente l'utilizzo del sito web per offrire marchi concorrenti di beni o servizi e non è comunque attivo sul mercato rilevante per la fornitura di servizi di intermediazione online per quanto riguarda tali beni o servizi.»

Sembrerebbe quindi che la Commissione sia soprattutto preoccupata dall'impatto delle piattaforme più grandi (Google, Apple, Facebook e Amazon – GAFA, come confermato da altri importanti provvedimenti emessi di recenti, quali ad esempio il Digital Market Act) e che non intenda invece perseguire le imprese più piccole (ad esempio i franchisor nell'esempio citato). Tuttavia, è essenziale che le imprese che intendano offrire tali servizi (ad esempio, alla propria rete di vendita) valutino accuratamente i possibili rischi e adottino tutele adeguate.

5. Obbligo di non concorrenza del distributore

Il nuovo Regolamento ha mantenuto la limitazione a cinque anni dell'obbligo di non concorrenza durante il periodo contrattuale, già previsto dal precedente VBER.
Tuttavia, il § 248 delle Linee Guida prevede che:
«.. Gli obblighi di non concorrenza che sono tacitamente rinnovabili oltre i cinque anni possono beneficiare dell'esenzione per categoria, purché l'acquirente possa effettivamente rinegoziare o risolvere l'accordo verticale contenente l'obbligo con un ragionevole preavviso e a un costo ragionevole, e sia quindi in grado di passare a un altro fornitore dopo la scadenza del periodo di cinque anni. ..»
Pertanto, ora gli accordi di distribuzione possono includere una clausola di tacito rinnovo, a condizione che siano rispettate le condizioni richieste dalla disposizione sopra citata.

6. Conclusioni

In questo articolo abbiamo trattato le principali novità del Regolamento 720/2022; vi sono ovviamente ulteriori aspetti che sono stati oggetto di riforma e che, nel contesto della verifica dei contratti, dovranno essere tenuti in considerazione. Inoltre, come anticipato, la valutazione della nuova disciplina può anche costituire l'occasione e l'opportunità per elaborare nuove strategie di riorganizzazione delle reti di vendita offline e online, nel contesto territoriale europeo.
Questo tema sarà anche oggetto di discussione e confronto nell'ambito della prossima conferenza annuale dell'International Distribution Institute (IDI) che si terrà il 9-10 giugno 2023, a Bologna.

Avv. Silvia Bortolotti
BBM Partners, Buffa, Bortolotti & Mathis