Jean Monnet Chair 2024-2027

DREAM-EU

Digital Rights Empowerment Across Market in the European Union

Co-funded by the European Union

DATABASE GIURISPRUDENZA

OTTOBRE-NOVEMBRE 2025

Protezione dei dati personali

Sentenza della Corte del 2 dicembre 2025, causa C-492/23, *Russmedia Digital e Inform Media Press*.

In base al regolamento generale sulla protezione dei dati (GDPR, regolamento (UE) 2016/679), il gestore di un sito di mercato *online* è responsabile del trattamento dei dati personali contenuti negli annunci pubblicati sulla sua piattaforma. Al riguardo, egli è tenuto ad individuare, prima della pubblicazione, gli annunci che contengono dati sensibili e a verificare che l'inserzionista corrisponda effettivamente alla persona i cui dati figurano nel relativo annuncio, a meno che esso disponga del consenso esplicito di tale persona. I fatti traggono origine dalla pubblicazione su un sito *internet* di proprietà di una società rumena, da parte di una persona non identificata, di un annuncio in cui si affermava la disponibilità di una donna (di cui venivano anche diffuse alcune foto e il numero di telefono) ad offrire servizi sessuali. Ritenendo tale annuncio lesivo dei propri diritti all'immagine, all'onore, alla reputazione e alla vita privata, nonché incompatibile con le norme relative al trattamento dei dati personali, la donna ha adito la giustizia rumena. In tale contesto, la Corte d'appello di Cluj ha chiesto alla Corte di giustizia di chiarire, da un lato, gli obblighi che gravano sul gestore di un mercato *online* ai sensi del GDPR, dall'altro, se tale gestore possa avvalersi dell'esonero da responsabilità previsto dall'art. 14, par. 1, della direttiva 2000/31/CE per i prestatori di servizi intermediari. Sotto il primo profilo, la Corte ha precisato che, sebbene formalmente inseriti da utenti terzi, gli annunci presenti su un sito *web* sono resi accessibili al pubblico grazie alla piattaforma: ne consegue che il gestore di un mercato *online* sia titolare, ai sensi dell'art. 4, punto 7, del GDPR, del trattamento dei dati personali contenuti negli annunci pubblicati sulla propria piattaforma. Perciò, qualora non ravvisi corrispondenza tra l'utente intenzionato a inserire un annuncio e la persona di cui siano resi noti i dati sensibili, il gestore di un mercato *online* deve rifiutare la pubblicazione dell'annuncio in questione. Sotto il secondo profilo, la Corte ha escluso che detto gestore possa sottrarsi a tali obblighi invocando l'esonero da responsabilità di cui all'art. 14 della direttiva 2000/31. Ciò perché, secondo il giudice dell'Unione, l'esenzione di cui il gestore potrebbe eventualmente beneficiare in relazione alle informazioni ospitate sul proprio sito non incidono sulla portata degli obblighi ad esso incombenti ai sensi del GDPR.

Responsabilità dei servizi intermediari di *hosting* ai sensi della direttiva 2000/31/CE

Conclusioni dell'Avvocato generale Maciej Szpunar del 27 novembre 2025, causa C-421/24, *AGCOM (gioco d'azzardo* online*)*.

Secondo l'Avvocato generale Szpunar, l'attività di un prestatore di servizi di *hosting* concernente la memorizzazione di video contenenti pubblicità di giochi d'azzardo rientra nell'ambito di applicazione della direttiva 2000/31/CE sul commercio elettronico. Tuttavia, in relazione ai contenuti illeciti pubblicati da soggetti terzi con i quali il prestatore abbia concluso un contratto di *partnership* commerciale, la deroga alla responsabilità del prestatore prevista dall'art. 14, par. 1, della direttiva, trova applicazione solo qualora il contratto sia stato formulato in modo tale da escludere il controllo dell'intermediario sui contenuti memorizzati sulla sua piattaforma. I fatti traggono origine dalla sanzione inflitta dall'Autorità per le garanzie nelle comunicazioni (AGCOM) a Google a causa dei video contenenti pubblicità di giochi con vincita in denaro pubblicati sul canale YouTube di un noto *creator*, con il quale Google aveva sottoscritto un contratto di *partnership* commerciale. Il Consiglio di Stato italiano, chiamato a risolvere la controversia tra le parti, ha promosso un rinvio pregiudiziale avente ad oggetto l'interpretazione di taluni profili della direttiva 2000/31/CE. Secondo l'Avvocato generale, il fatto che una piattaforma memorizzi video contenenti pubblicità di giochi d'azzardo non significa che essa operi nel settore del gioco d'azzardo. Di conseguenza, dal momento che l'art. 1, par. 5, lett. *d*), esclude dall'ambito di applicazione della direttiva l'offerta dei giochi di fortuna, tale esclusione non rileva in riferimento ai fornitori dei servizi di *hosting*, come YouTube, che ospitino contenuti volti a promuovere tali giochi. Per quanto riguarda, invece, il regime di esenzione dalla responsabilità sancito dall'art. 14, par. 1, al fine di verificarne l'applicabilità, occorre valutare, secondo Szpunar, se l'attività del prestatore di servizi abbia una natura meramente tecnica, oppure comporti una forma di controllo diretto sui contenuti caricati dai soggetti terzi, il quale può concretizzarsi, ad esempio, nella partecipazione alla redazione e alla selezione delle pubblicazioni, nonché alla loro ottimizzazione. Viceversa, il fatto che un prestatore sia remunerato per tali servizi, si attivi per individuare i contenuti illeciti, o offra talune funzioni di ottimizzazione delle visualizzazioni sulla sua piattaforma, non è sufficiente ad escludere l'applicazione dell'art. 14 della direttiva.

Conservazione di dati biometrici e genetici

Sentenza della Corte del 20 novembre 2025, causa C-57/23, *Policejní prezidium*.

Il diritto dell'Unione europea non osta a una normativa nazionale che consenta alle autorità di polizia di conservare i dati biometrici e genetici di una persona perseguita penalmente o sospettata di aver commesso un reato. Peraltro, purché siano previsti termini adeguati volti a verificare periodicamente la stretta necessità di conservare tali dati, non è indispensabile che la normativa nazionale stabilisca un periodo massimo di conservazione. Il caso traeva origine dal rinvio pregiudiziale sollevato dalla Corte amministrativa suprema della Repubblica Ceca volto a verificare la compatibilità della legge nazionale relativa alla polizia con la direttiva (UE) 2016/680. In particolare, un funzionario pubblico, condannato in via definitiva per abuso di potere, contestava la legittimità delle misure di identificazione adottate dalla polizia nell'ambito del procedimento penale a suo carico, nonché la conservazione dei dati ottenuti, ritenendole un'illegittima ingerenza nella sua vita privata. Nello specifico, la polizia aveva ordinato il rilevamento delle sue impronte digitali, un prelievo orale dal quale aveva ricavato un profilo genetico, la realizzazione di fotografie e la redazione di una descrizione della sua persona. Innanzitutto, la Corte di giustizia ha stabilito che l'art. 6 della direttiva 2016/680 non vieta la raccolta di dati biometrici e genetici di qualsiasi persona perseguita per aver commesso un reato doloso o sospettata di aver commesso un tale reato, purché le finalità della raccolta non impongano di operare una distinzione tra queste due categorie di persone. In secondo luogo, alla luce dell'art. 10 della direttiva, il quale prevede che il trattamento dei dati personali sensibili, tra cui i dati biometrici e genetici, debba risultare «strettamente necessario», la Corte precisa che le finalità di tale trattamento, da un lato, debbano essere definite in modo sufficientemente preciso da consentire di verificare il rispetto della condizione della necessità, dall'altro, non possano essere conseguite in modo altrettanto efficace facendo ricorso a categorie diverse di dati.

Qualificazione di una «piattaforma *online* di dimensioni molto grandi» ai sensi del DSA

Sentenza del Tribunale del 19 novembre 2025, causa T-367/23, *Amazon* c. *Commissione*.

Il Tribunale ha respinto il ricorso presentato da Amazon avverso la decisione della Commissione volta a qualificare la piattaforma "Amazon Store" come «piattaforma *online* di dimensioni molto grandi» ai sensi dell'art. 33, par. 4, del DSA. A fondamento del proprio ricorso, la ricorrente eccepiva, in forza dell'art. 277 TFUE, l'illegittimità dell'art. 33, par. 1, del DSA, in quanto lesivo di taluni diritti tutelati dalla Carta dei diritti fondamentali, nella misura in cui impone ai mercati *online* di grandi dimensioni di rispettare taluni obblighi supplementari in materia di gestione dei rischi sistemici, previsti dagli artt. 34-43. Innanzitutto, secondo il Tribunale, sebbene gli obblighi previsti dal DSA costituiscano un'ingerenza nella libertà d'impresa (art. 16 della Carta) delle piattaforme, tale ingerenza non è sproporzionata poiché siffatti obblighi, da un lato, non impediscono l'esercizio dell'attività imprenditoriale dei fornitori delle piattaforme, dall'altro, sono finalizzati ad evitare che le piattaforme di grandi dimensioni, potendo raggiungere un grande numero di utenti, possano favorire la diffusione di contenuti illeciti tali da costituire rischi sistemici per la società. Ragion per cui, peraltro, non operando una differenziazione arbitraria o manifestamente inadeguata, bensì calibrata alla luce dei potenziali rischi sistemici che le piattaforme di grandi dimensioni possono comportare, il regime specifico, e più gravoso, previsto per tali tipologie di piattaforme in ragione del loro numero di utenti non è incompatibile con il principio della parità di trattamento (art. 20 della Carta). Parimenti salvaguardato sarebbe il diritto di proprietà (art. 17, par. 1, della Carta), poiché il DSA si limita ad imporre oneri amministrativi in capo ai fornitori delle piattaforme, senza privarli della proprietà di queste ultime. Per quanto attiene alla libertà di espressione di informazione (art. 11, par. 1, della Carta), l'obbligo imposto alle piattaforme di assicurare un sistema di raccomandazione non basato sulla profilazione, pur avendo l'effetto di limitare il modo in cui i prodotti commercializzati sono presentati, non è lesivo della libertà di espressione, perseguendo, al contempo, un obiettivo di interesse generale, quale la tutela dei consumatori. Venendo, infine, all'eventuale violazione del diritto al rispetto della vita privata (art. 7 della Carta), il Tribunale ritiene che gli obblighi di trasparenza pubblicitaria e di accesso dei ricercatori a determinati dati rispondano a un obiettivo di interesse generale, ossia la prevenzione dei rischi sistemici nell'ottica di contribuire a un elevato livello di tutela dei consumatori.

Diritto alla protezione dei dati personali

Conclusioni dell'Avvocato generale Laila Medina del 23 ottobre 2025, cause riunite C-258/23, C-259/23 e C-260/23, *Imagens Médicas Integradas*, *Synlabhealth II*, *Sociedade Gestora de Participações Sociais e a.*

I casi traevano origine da una causa pendente dinanzi a un giudice portoghese, chiamato a valutare la legittimità di un sequestro, effettuato dall'autorità nazionale garante della concorrenza, di alcuni messaggi di posta elettronica scambiati tra gli impiegati delle società sottoposte a un'indagine vertente su presunte violazioni della normativa in materia di concorrenza. Secondo le società interessate, tale sequestro era avvenuto in violazione del loro diritto al segreto della corrispondenza, in quanto avrebbe dovuto essere autorizzato dal giudice istruttore. La questione sollevata dal giudice portoghese investito delle cause è volta a chiarire se la nozione di «corrispondenza», la cui inviolabilità è un diritto fondamentale che beneficia di un livello di protezione più elevato, includa le comunicazioni contenute nella posta elettronica di servizio dei dipendenti. L'Avvocato generale Medina si era già pronunciata sulla questione in data 20 giugno 2024, sostenendo che il diritto al rispetto della vita privata e familiare sancito dall'art. 7 della Carta dei diritti fondamentali non osti alla legislazione di uno Stato membro che consenta all'autorità nazionale garante della concorrenza di procedere, in assenza di una previa autorizzazione giudiziaria, al sequestro di messaggi di posta elettronica. Nel frattempo, però, la Corte si è pronunciata nella sentenza *Landeck* (causa C-548-21), precisando che l'accesso ai dati personali contenuti in un telefono cellulare per finalità investigative debba essere assoggettato al previo controllo di un giudice o di un'entità amministrativa indipendente, fatta eccezione per i casi di urgenza. A seguito di ciò, l'Avvocato generale è stato invitato dalla Corte a verificare se la risposta al quesito sollevato dal giudice portoghese debba tenere conto della sentenza *Landeck*. A suo avviso, la giurisprudenza in questione non è trasponibile ai casi di specie, giacché i sequestri effettuati non configurano una raccolta illimitata di dati personali poiché i dati raccolti, essendo finalizzati a individuare pratiche anticoncorrenziali nel mercato interno, sono circoscritti alle informazioni commerciali aventi un nesso con le pratiche oggetto di indagine. Inoltre, l'ampiezza dei dati ricavabili dai messaggi di posta elettronica scambiati in un contesto lavorativo, a differenza di quelli ricavabili da un telefono cellulare, non è tale da restituire una descrizione dettagliata e approfondita della vita privata della persona interessata. Ne consegue che, rispettando tali requisiti di proporzionalità, la fattispecie oggetto di controversia dinanzi al giudice portoghese sia compatibile con il rispetto del contenuto essenziale del diritto alla protezione dei dati personali di cui all'art. 8, par. 2, della Carta. Secondo Medina, infine, il sequestro contestato dovrebbe esser preceduto da un'autorizzazione giudiziaria solo qualora venisse effettuato presso il domicilio privato di una persona o al fine di incriminare penalmente una persona fisica.