# Consenso *bis*: la Corte di giustizia torna sui requisiti di un valido consenso privacy

Maria Chiara Meneghetti

**Corte di giustizia dell'Unione europea, 11 novembre 2020, C-61/19, *Orange România SA contro Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)***

Spetta al titolare del trattamento dimostrare la raccolta di un consenso valido e informato.
Una clausola contrattuale secondo cui l'interessato è stato informato e ha acconsentito alla raccolta dei suoi dati non è idonea a dimostrare la valida manifestazione di volontà dell'interessato se (i) è stata preselezionata dal titolare; (ii) induce in errore l'interessato circa la necessità del consenso per la stipulazione del contratto; (iii) la libera scelta di opporsi al trattamento è pregiudicata dall'esigenza per l'interessato di negare attivamente il proprio consenso mediante la compilazione di un modulo.

## Sommario



## Keywords

consenso – libertà – protezione dei dati personali – autodeterminazione – Corte di giustizia

## 1. Introduzione

La sentenza in commento vede la Corte di giustizia dell'Unione europea nuovamente alle prese con una tematica centrale nella disciplina in materia di protezione dei dati personali: la validità del consenso prestato dall'interessato. Il consenso rappresenta una delle diverse condizioni di liceità – i.e. "basi giuridiche" – che il diritto europeo pone a fondamento di un legittimo trattamento di dati personali. Non tutti gli atti affermativi sono considerati giuridicamente validi e permettono quindi al titolare di raccogliere e utilizzare i dati del consenziente, ma solo quelli che soddisfano una serie di requisiti. Dalla direttiva "madre" 95/46/CE ("Direttiva"), passando per le autorità garanti nazionali, fino al regolamento (UE) 2016/679 ("Regolamento"), l'evoluzione del consenso come presupposto giuridico di un lecito trattamento ha infatti dimostrato

la necessità di individuare specifiche condizioni che assicurino la sua effettività del e garantiscano la libera e incondizionata manifestazione di volontà dell'individuo.
La sentenza *Orange România* rappresenta quindi la seconda occasione della Corte, che segue la precedente sentenza nella causa C-673/17 *Planet49*[1], di fare chiarezza sulle condizioni che la Direttiva, prima, e il Regolamento, oggi, richiedono affinché un consenso possa dirsi validamente espresso. A differenza della prima sentenza, in cui la Corte aveva esaminato la prestazione del consenso nel mondo digitale[2], la presente vicenda si svolge interamente nel mondo analogico, avendo ad oggetto la raccolta del consenso mediante clausole standard stampate su moduli contrattuali. Il mezzo digitale o analogico non influisce in realtà sulle conclusioni della Corte, che rimangono tecnologicamente neutre e analogicamente applicabili a entrambe le realtà.
Il consenso non è, come si è detto, l'unico presupposto che il titolare del trattamento può adoperare per raccogliere e utilizzare legittimamente i dati personali. La Direttiva, come anche il Regolamento, elencano altri cinque presupposti alternativi (adempimento contrattuale o normativo, interesse pubblico, legittimo interesse, tutela degli interessi vitali), in presenza dei quali il trattamento può essere effettuato in assenza dell'autorizzazione espressa dell'interessato. Eppure, il requisito del consenso è da sempre ritenuto un tratto essenziale e caratteristico della disciplina in materia di trattamenti di dati e rimane profondamente legato alla dinamica evolutiva di uno dei diritti che tale disciplina intende tutelare, ossia il diritto alla protezione dei dati personali.
Negli atti internazionali che per primi indicano alcuni principi generali in materia di trattamento dei dati personali, il consenso non aveva una posizione di particolare rilievo. La Convenzione 108 del Consiglio d'Europa (1981)[3] non conteneva alcuna menzione del consenso dell'interessato tra le sue disposizioni, mentre lo stesso faceva una comparsa all'interno delle Linee Guida dell'OCSE (1980)[4], senza tuttavia ricevere particolari approfondimenti. Analogamente, le leggi nazionali di "prima generazione" [5],

[1] Sentenza della CGUE, C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV contro Planet49 GmbH*, 1° ottobre 2019 (di seguito "*Planet 49*").

[2] Nella causa *Planet49*, la controversia verteva sulla validità del consenso degli utenti ottenuto mediante una casella di spunta preselezionata. La società *Planet49* aveva organizzato un gioco a premi *online,* a cui gli utenti potevano iscriversi comunicando il loro nome e indirizzo in una pagina web. Nella stessa pagina erano presenti delle caselle da selezionare, tra cui una *check box* che autorizzava l'installazione di cookie di profilazione sul terminale del partecipante. Quest'ultima risultava però già preselezionata, cosicché in assenza di de-selezione da parte dell'utente, l'autorizzazione sarebbe stata prestata automaticamente. La CGUE, interpellata dalla Corte federale di giustizia (*Bundesgerichtshof*), ritiene che il consenso così raccolto (c.d. *opt-out*) non possa ritenersi validamente espresso, in quanto non soddisfa i requisiti previsti dal Regolamento, in particolare l'inequivocabilità della sua prestazione. Per una disamina della sentenza *Planet49*, si rinvia in *questa Rivista* a R. Cabazzi, *Utilizzo dei cookie e (nuova) tutela dell'utente interessato: la presa di posizione della Corte di Giustizia nel caso Planet49,* 2, 2020, 316 ss.

[3] Trattato n. 108 del Consiglio d'Europa, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, Strasburgo, 28 gennaio 1981.

[4] *Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti di informazione: verso una cultura della sicurezza*, 1980. Le Linee Guida sono state aggiornate nel 2013.

[5] Sono le prime leggi che parlano di dati personali e ne regolano il trattamento, emanate nei primi anni'70 in particolare dallo stato di Hessen in Germani (*Hessische Datenschutzgesetz*) nel 1970, in Svezia (*Datalagen*) nel 1973. Per una disamina del perscorso evolutivo delle legislazioni privacy si rinvia a F.W. Hondius, *Emerging data protection in Europe*, Amsterdam 1975; R. Pagano, *Panorama of Personal Data Protection Laws*, in *Council of Europe, Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the*

volte a regolare i trattamenti automatizzati di dati e nate principalmente in risposta alla creazione di banche dati governative centralizzate, avevano obiettivi di tutela collettiva che non lasciavano posto alle scelte consensuali individuali[6]. Il consenso ha iniziato a imporsi come elemento centrale nella disciplina dei trattamenti contestualmente all'emersione di un diritto alla protezione dei dati personali, interpretato come diritto positivo alla "autodeterminazione informativa"[7], ossia il diritto dell'individuo di «mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata»[8]. Lo sviluppo tecnologico e l'avvento dell'informatica di massa hanno infatti portato il diritto alla privacy, originariamente inteso come diritto alla protezione della sfera privata del cittadino dalle interferenze dello Stato e poi, più in generale, dalle intrusioni altrui, a trasformarsi progressivamente in un diritto di controllo e gestione della circolazione delle proprie informazioni[9]. È in questo contesto che il consenso della persona interessata, conferendo al singolo il potere di autorizzare, in questo senso determinare, ciò che viene fatto delle proprie informazioni, è diventato uno dei principali strumenti di controllo per l'attuazione dell'autodeterminazione personale. Questo mutamento di paradigma, che valorizza la dimensione dinamica del diritto alla protezione dei dati personali e fa dell'individuo attore protagonista nel suo esercizio, ha iniziato ad affermarsi già nelle normative privacy nazionali adottate verso la fine degli anni '70, dove il consenso dell'interessato ha incominciato in alcuni casi a comparire come prerequisito per l'esecuzione dei trattamenti[10]. L'adozione della diret-

*development and application of legislation on data protection*, 1983, Rome, Camera dei Deputati; G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Switzerland, 2014.

6 V. Mayer-Schoönberger, *Generational development of data protection in Europe*, Cambridge, 1997, 223.

7 Il diritto alla "autodeterminazione informativa" viene coniato e riconosciuto per la prima volta dalla Corte costituzionale tedesca, in una storica sentenza del 1983 (*Volkszählungsurteil, Bundesverfassungsgericht* 15-12-1983, 1 BvR 209/83). A fare da sfondo, la richiesta rivolta alla Corte di decidere sulla costituzionalità della legge sul censimento emanata l'anno prima. Il cuore della sentenza è invece l'articolato ragionamento della Corte che, muovendo dal diritto alla dignità e al libero sviluppo della personalità, afferma l'esistenza di un diritto dei singoli di autodeterminarsi stabilendo in modo libero e autonomo a chi, come e quanto condividere delle proprie informazioni. Viene sancito così il diritto di ogni individuo alla autodeterminazione informativa (*das informationelles Selbstbestimmungsrech*), che deve essere tutelato di fronte a moderne tecnologie che, alterando il grado di controllo sulla circolazione delle informazioni, posso pregiudicare libero sviluppo della personalità degli individui. Sul tema, si veda G. Sartor, *Tutela della personalità e normativa per la "protezione dei dati". La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del Datenschutz,* in *Informatica e Diritto*, 12, 1986, 95 ss.

8 S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, 122.

9 Vasta è la letteratura sull'evoluzione del diritto alla privacy, in prospettiva comparatistica e nazionale. Si rinvia a S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.,* 1997, 583 ss.; Id., *Intervista su privacy e libertà*, Bari-Roma, 2005; G. Buttarelli, *Banche dati e tutela della riservatezza,* Milano, 1997; V. Cuffaro-V. Ricciuto-V. Zeno Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998; G. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012.

10 A partire dalla fine anni '70, diversi stati europei iniziano a adottare proprie legislazioni in materia di privacy tra cui Francia (*Loi informatique e libertés*), Austria (*Datenschutzgesetz*), Norvegia (*Lov om folkeregistrering*) e Danimarca (*Lov om private registre* e *Lov om offentlige myndigheders registre*) nel 1978. Queste legislazioni che di "seconda generazioni" si inizia ad apprezzare uno shift verso una dimensione più individuale dell'esercizio del diritto alla protezione dei dati personali. In alcune di queste il consenso inizia già a presentarsi come presupposto per il trattamento (v. legge norvegese). Questo cambiamento diventa sempre più evidente nelle legislazioni successive, tra cui quelle di Finlandia (1987), Portogallo

tiva 95/46/CE, che parte dai principi internazionali della Convenzione 108 e fa proprie le esperienze nazionali, ha sancito l'ingresso ufficiale del consenso tra le condizioni di liceità al trattamento dei dati personali previste all'interno della disciplina europea. Il recepimento della Direttiva nelle normative nazionali ha rafforzato in maniera evidente il ruolo del consenso quale regola generale per il trattamento dei dati[11]. Cinque anni più tardi, il consenso ha trovato espressa menzione nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea, che, dopo aver stabilito il diritto di ogni persona alla tutela dei propri dati personali, richiede che gli stessi siano «trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge».

Negli anni che hanno seguito il recepimento della Direttiva, caratterizzati da un'accelerazione tecnologica e digitale, la funzione di controllo affidata allo strumento consensuale è stata progressivamente erosa a fronte di un utilizzo eccessivo e distorto di tale meccanismo. L'aumento della domanda di dati accompagnato dalla percezione che il consenso una volta ottenuto – indipendentemente dalle modalità – potesse giustificare in maniera generalizzata qualsiasi trattamento di dati personali hanno portato alla proliferazione di formule di consenso "vuote", ridotte a meri formalismi e ben lontani dall'idea di autodeterminazione con cui il consenso era nato.

Allo snaturamento del consenso tentano di mettere un freno le autorità di protezione dei dati, ribadendo e precisando i criteri di libertà, specificità e inequivocabilità che la Direttiva madre e le normative nazionali richiedevano affinché il consenso potesse ritenersi validamente prestato e quindi legittimo[12]. I diversi interventi hanno trovato, infine, collocazione all'interno del regolamento (UE) 2016/679. Quest'ultimo non fa espresso riferimento a un diritto all'"autodeterminazione informativa", ma richiama la centralità dell'individuo, ritenendo opportuno che «le persone fisiche abbiano il controllo dei dati personali che le riguardano» (considerando 7). Nel Regolamento il legislatore adotta un approccio rigoroso: la definizione di consenso diventa più dettagliata, è introdotto un articolo (art. 7) e diversi considerando che ne descrivono in maniera pratica e analitica le condizioni di validità e le regole in merito al relativo onere probatorio, ed è previsto un articolo *ad hoc* (art. 8) in materia di consenso dei minori in relazione ai servizi della società dell'informazione.

(1991), Spagna e Belgio (1992). V. Mayer-Schönberger, *Generational development*, cit., 227 ss. e G. González Fuster, *The Emergence of Personal Data,* cit., 147-156, L.A.Bygrave, *Data protection law: Approaching its rationale, logic and limits*, The Hague, 2002.

[11] La l. 675/1996, legge di recepimento in Italia della Direttiva madre, e il successivo d.lgs. 196/2003, Codice Privacy, che riorganizza in maniera organica l'intera disciplina, il consenso ricopre una posizione di preminenza rispetto alle altre basi giuridiche che vengono considerate sue "eccezioni" (v. art. 23 "Consenso" e art. 24 "Casi nei quali può essere effettuato il trattamento senza consenso" del Codice Privacy antecedente le modifiche effettuate dal decreto di adeguamento d.lgs. 101/2018).

[12] Si veda in particolare il Parere 15/2011 del Gruppo di lavoro Art. 29 sulla definizione di consenso (WP187) e il Parere 06/2014 del Gruppo di lavoro Art. 29, sul consenso esplicito quale base giuridica per il trattamento delle categorie sensibili di dati. Sui limiti del consenso anche il *Working Document on the processing of personal data relating to health in electronic health records* (WP 131), il Parere 08/2001 del Gruppo di lavoro Art. 29 sul trattamento dei dati nel contesto lavorativo (WP48), e il secondo Parere 04/2009 sul trattamento dei dati da parte della World Anti-Doping Agency (WADA) (WP 162).

## 2. La vicenda

I fatti oggetto delle due questioni pregiudiziali sottoposte alla Corte di giustizia traggono origine da una controversia tra un fornitore di servizi di telecomunicazioni (Orange România SA) e l'autorità nazionale per la protezione dei dati personali rumena (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, "ANSPDCP") in merito agli obblighi del provider rispetto alla raccolta e conservazione di copie di un documento di identità dei propri clienti, all'atto di sottoscrizione del contratto di fornitura.

Ai sensi della legge rumena in materia di protezione dei dati personali in vigore al momento della vicenda (legea n. 677/2001), il trattamento di un codice numerico personale o di altri dati personali con una funzione di identificazione di portata generale (es. la carta di identità) poteva essere effettuato solo se l'interessato avesse prestato espressamente il suo consenso[13]. Sulla base di tale norma, la ANSPDCP contestava e sanzionava la Orange România per non aver dimostrato che i suoi clienti avevano compiuto una scelta informata relativamente alla raccolta e alla conservazione di copie dei loro documenti d'identità.

I contratti conclusi tra il provider e i propri clienti contenevano una formula standard, che indicava che i clienti erano stati informati e avevano espresso il loro consenso alla raccolta e alla conservazione di una copia della propria carta d'identità. La sussistenza del consenso dei clienti veniva documentata tramite l'apposizione di un segno in una casella presente nella documentazione contrattuale, che veniva tuttavia apposto non dal cliente/interessato ma da un agente di vendita del provider, dopo aver informato oralmente i clienti del contenuto della clausola e in ogni caso prima della sottoscrizione del contratto stesso. Da quanto emerso in sede di giudizio di rinvio davanti al Tribunalul Bucureşti (Tribunale superiore di Bucarest, Romania), in alcuni casi il segno nella casella rispecchiava la reale scelta del cliente, mentre in altri casi - pur in presenza del segno di spunta - i clienti avevano invece negato tale trattamento. Inoltre, dalle policy interne della società si evinceva che il rifiuto alla conservazione della copia del documento di identità era stato documentato mediante compilazione di un modulo specifico allegato al contratto stesso[14].

Alla luce dei fatti, il giudice del rinvio decide quindi di rimettere alla Corte di giustizia due questioni pregiudiziali volte a chiarire le condizioni che devono essere soddisfatte per poter considerare una manifestazione di volontà (i) specifica e informata; (ii) liberamente espressa.

[13] Art. 8 della legea n. 677/200 rubricato "Trattamento di dati personali aventi funzione identificativa" nel quale si leggeva «Il trattamento del codice numerico personale o di altri dati personali che hanno una funzione di identificazione di portata generale può essere effettuato solo se: a) la persona interessata ha fornito espressamente il suo consenso; oppure b) il trattamento è previsto espressamente da una disposizione di legge».

[14] Sui fatti della vicenda, v. le conclusioni dell'Avvocato generale Maciej Szpunar presentate il 4 marzo 2020, §§ 12-20 e la sentenza *Orange România*, cit., §§ 20-26.

## 3. Tra Direttiva e Regolamento

In via preliminare, è utile accennare brevemente alla normativa che la Corte ritiene applicabile alla fattispecie in esame. Come anticipato, l'ANSPDCP adotta il proprio provvedimento sulla base del diritto rumeno in vigore al momento dei fatti, la l. 677/2001, che rappresentava normativa nazionale di recepimento della Direttiva madre. La sanzione è adottata infatti il 28 marzo 2018, poco prima dell'entrata in vigore del Regolamento, che porta a una revisione adeguatrice della legislazione interna ad opera della legea 190/2018. Le questioni pregiudiziali promosse dal giudice del rinvio vertono quindi correttamente sull'interpretazione delle caratteristiche del consenso, come previste dalla Direttiva madre.

Tuttavia, come già avvenuto in precedenti occasioni[15], sia l'Avvocato generale, sia la Corte decidono di estendere il proprio raggio di valutazione alle previsioni del Regolamento, con l'intento di fornire indicazioni interpretative di maggiore attualità. A tal fine, rilevano come l'autorità garante rumena non si sia limitata a infliggere un'ammenda al provider, ma abbia emesso un'ingiunzione per la distruzione delle copie dei documenti d'identità in oggetto, che era stata sospesa nelle more del giudizio e avrebbe prodotto i suoi effetti nel futuro, nel vigore del nuovo Regolamento[16]. Ritengono quindi che le domande poste dal giudice debbano trovare risposta sulla base tanto della Direttiva, quanto del Regolamento.

È evidente che la definizione e le caratteristiche di validità del consenso hanno subito un'evoluzione dalla Direttiva al Regolamento. L'art. 2, lett. *h),* della Direttiva definiva il consenso della persona interessata «qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento», mentre il successivo art. 7 (che elencava le diverse basi giuridiche) specificava la forma "inequivocabile" con cui il consenso dovesse essere prestato. Il Regolamento contiene una definizione di consenso più articolata, che viene ulteriormente arricchita dai considerando. In particolare, ai sensi dell'art. 4, n. 11, del Regolamento, il consenso diventa «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento», mentre l'art. 7 letto in combinato disposto con il considerando 32 del Regolamento ne specifica in maniera puntuale alcuni tratti caratteristici (es. specificità e libertà, nonché chiarimenti sull'onere probatorio). Come sottolineato dall'Avvocato generale, le differenze terminologiche tra i due testi risultano più apparenti che sostanziali[17]. Il Regolamento infatti esplicita o precisa condizioni di validità del consenso che erano già presenti, seppur accennate, all'interno della Direttiva (es. l'inequivocabilità), o in ogni caso recepisce le ormai consolidate posizioni interpretative già espresse dalle autorità garanti nazionali, singolarmente e congiuntamente nell'allora Gruppo di lavoro Art. 29.

Nell'ambito delle precisazioni introduttive, è interessante anche il breve inciso dell'Av-

[15] Nel medesimo senso si era espressa la Corte nella sentenza *Planet49,* cit., § 41.

[16] Sentenza *Orange România*, cit., § 31.

[17] Conclusioni dell'Avvocato generale, cit., §§ 38-42.

vocato generale che, nell'intento di circoscrivere il perimetro entro cui la Corte è chiamata a rispondere, precisa il rapporto tra due basi giuridiche. In particolare, l'Avvocato generale chiarisce come non sia oggetto della causa la questione se il provider possa esigere dai suoi clienti, ai fini di identificazione degli stessi, la produzione e conservazione della carta d'identità nell'ambito della sottoscrizione contrattuale. In altre parole, l'Avvocato puntualizza come non sia oggetto di discussione la base giuridica adottata dal provider (consenso) ovvero la possibilità per lo stesso di utilizzare una diversa base legale (adempimento contrattuale) per far valere le proprie ragioni. In effetti, l'interpretazione dei fatti in oggetto alla luce delle nuove disposizioni introdotte dal Regolamento avrebbe potuto – astrattamente – aprire nuovi spiragli di contestazione. Con riguardo al trattamento dei dati contenuti in documenti identificativi, mentre la Direttiva, come trasposta nella legge nazionale di riferimento, imponeva sostanzialmente al provider la raccolta del consenso dell'interessato, la nuova norma di raccordo nazionale, la legea 190/2018, rimette ora al titolare la scelta della base giuridica più appropriata tra quelle offerte dall'art. 6, par. 1, del Regolamento (quindi anche l'adempimento contrattuale)[18]. L'Avvocato sottolinea però come sebbene possa ritenersi legittimo richiedere un documento ai fini dell'identificazione del cliente per la prestazione di un servizio, «esigere che un cliente accetti la produzione di copie e la conservazione dei propri documenti di identità» risulta «tuttavia, eccedere quanto necessario per l'adempimento del contratto»[19]. Elimina quindi ogni dubbio sul fatto che il consenso sia l'unica base giuridica di cui avrebbe potuto valersi la società per il trattamento in oggetto.

## 4. La validità del consenso e l'onere probatorio

Le due questioni pregiudiziali presentate impongono alla Corte di valutare se un contratto relativo alla fornitura di servizi di telecomunicazioni che contiene una clausola secondo la quale la persona interessata è stata informata e ha acconsentito alla raccolta e alla conservazione di una copia del suo documento di identità a fini di identificazione sia idoneo a dimostrare che tale persona ha prestato validamente il proprio consenso, nell'accezione congiunta della Direttiva e del Regolamento, a tale raccolta e conservazione.

Il percorso logico seguito dalla Corte ripercorre sostanzialmente i requisiti che le due norme impongono affinché la manifestazione di volontà della persona interessata possa considerarsi validatamente prestata.

Interpretando congiuntamente le definizioni di consenso contenute nel Regolamento e nella Direttiva, la Corte prende le mosse dal requisito di "inequivocabilità". Una manifestazione di volontà inequivocabile può dirsi tale solo in presenza di un comportamento attivo dell'interessato o come esplicitamente previsto dal Regolamento di una

[18] Art. 4 della legea 190/2018, rubricato "Trattamento di un numero di identificazione nazionale" che recita «Il trattamento di un numero di identificazione nazionale, anche attraverso la raccolta o la divulgazione dei documenti che lo contengono, può essere effettuato nelle situazioni previste dall'art. 6 par. 1 del Regolamento generale sulla protezione dei dati».

[19] Cfr. conclusioni dell'Avvocato generale, cit., § 58.

«dichiarazione o azione positiva»[20]. Si richiede quindi che la persona interessata abbia effettuato un'azione deliberata per acconsentire al trattamento specifico. A tal riguardo, il considerando 32 del Regolamento esclude espressamente che configuri consenso «il silenzio, l'inattività o la preselezione di caselle». In tema di caselle preselezionate, la Corte si era espressa nella causa *Planet49* ritenendo praticamente impossibile determinare in modo oggettivo se, non deselezionando una casella preselezionata, l'utente di un sito Internet avesse inteso manifestare il proprio consenso al trattamento dei suoi dati personali. Tale modalità di raccolta del consenso, non potendo considerarsi un atto inequivocabile dell'individuo, non rispondeva alle condizioni di un valido consenso[21]. Analogamente, manca di inequivocabilità in termini privacy l'accettazione globale delle condizioni generali di contratto/servizio, in quanto non può essere considerata come un'azione positiva univoca ai fini del consenso all'utilizzo dei dati personali[22] (v. *infra* anche in tema di trasparenza).

La Corte passa poi ad esaminare i requisiti di "specificità" e "libertà", due ulteriori tratti fondamentali del consenso.

La prima condizione mira ad assicurare all'individuo un controllo granulare rispetto alle finalità specifiche per cui il consenso viene richiesto. In linea con il principio generale di "limitazione delle finalità"[23], ciascuna prestazione di consenso può essere infatti associata a una sola finalità di trattamento. Il requisito di specificità è quindi strettamente correlato a quello di "granularità", posto a tutela della libertà del consenso (come descritta *infra*), e di "trasparenza", principio generale che si traduce nella necessità che la persona interessata sia stata adeguatamente informata prima di acconsentire a un trattamento. Come ricorda la Corte, è obbligo del titolare mettere a disposizione dell'interessato le informazioni rilevanti (c.d. informativa privacy) rispetto al trattamento che intende effettuare, in un linguaggio chiaro, semplice e comprensibile, in modo tale che l'eventuale accettazione sia prestata con totale cognizione di causa[24]. Fornire informazioni agli interessati prima di ottenerne il consenso è fondamentale per consentire loro di capire a cosa stanno acconsentendo, di valutarne le conseguenze e, nel caso, di negare il proprio consenso[25]. Il medesimo principio di chiarezza, semplicità e accessibilità deve trovare applicazione anche con riferimento al linguaggio utilizzato nella formula di consenso[26], nonché nelle modalità stesse di presentazione della clau-

[20] Sentenza *Orange România*, cit., §§ 35-36.

[21] Sentenza *Planet49*, cit., §§ 55 e 57.

[22] Offrono utili chiarimenti sulle caratteristiche richieste per la validità del consenso privacy le *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, adottate dall'European Data Protection Board (EDBP) il 4 maggio 2020 ("Linee guida dell'EDPB"), spec. 20.

[23] L'art. 5 del Regolamento, che elenca i principi fondamentali applicabili a tutti i trattamenti di dati personali, individua al par. 1, lett. *b*), il principio di "limitazione delle finalità" ai sensi del quale i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità».

[24] Sentenza *Orange România*, cit., § 40; in precedenza già sentenza *Planet49*, cit., § 74.

[25] Sul requisito di consenso informato, si vedano le Linee guida dell'EDPB, cit., spec. 16-18.

[26] Così precisa il considerando 42 del Regolamento che, richiamando la direttiva 93/13/CEE del Consiglio concernente le clausole abusive nei contratti stipulati con i consumatori, ritiene opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole

sola. Indipendentemente dalla forma elettronica o cartacea, quando il consenso viene richiesto nell'ambito di un contratto, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie oggetto di contrattazione[27]. Deve quindi essere separata e distinta, e non può semplicemente figurare in un paragrafo all'interno delle condizioni generali di contratto.

Infine, la libertà del consenso richiede che l'interessato abbia una scelta effettiva di controllo sui propri dati. Il requisito di libertà, fondamentalmente legato al concetto di autonomia individuale, è il carattere che rappresenta in maniera più evidente la funzione di controllo sulla circolazione delle informazioni che la normativa conferisce al consenso. Se l'interessato non dispone di una scelta effettiva o si sente obbligato ad acconsentire oppure subisce conseguenze negative se non acconsente, il meccanismo consensuale non è in grado di operare correttamente perché impedisce all'individuo di autodeterminarsi in maniera incondizionata[28]. Dunque qualsiasi azione di pressione o influenza inappropriata sull'interessato, che impedisca a quest'ultimo di esercitare il suo libero arbitrio, rende il consenso invalido. Tra i fattori che possono influenzare il comportamento dell'interessato, sono stati da tempo individuati[29]: (i) lo squilibrio di potere, che comporta la soggezione dell'interessato nei rapporti con l'autorità pubblica o nel rapporto datore di lavoro/dipendente; (ii) la condizionalità, ossia il caso in cui la fornitura di un contratto o servizio sia subordinata al consenso al trattamento di dati personali che non sono necessari per l'esecuzione del contratto o servizio; (iii) il pregiudizio, ossia l'inganno, l'intimidazione, la coercizione o la prospettazione di conseguenze negative significative in caso di mancato consenso; e (iv) la granularità, connessa al requisito di specificità sopra descritto. In presenza di uno di tali fattori, il consenso si presume non essere stato prestato liberamente e sarà onere del titolare dimostrare il contrario.

Nel caso in esame, la presenza di tutti requisiti sopra accennati è contestata o quantomeno messa in discussione dalla Corte.

In primo luogo, la Corte solleva dubbi in merito all'inequivocabilità del consenso prestato. Rileva, infatti, come la casella relativa alla clausola con cui si indicava che i clienti fossero stati informati e avessero manifestato il consenso alla conservazione di una copia del loro documento d'identità fosse stata selezionata dagli agenti di vendita della società, prima che tali clienti procedessero alla firma dell'intero contratto[30]. La presenza di una spunta all'interno della casella non viene considerata elemento idoneo a dimostrare una manifestazione positiva del consenso dei clienti, soprattutto in assenza di indicazioni che confermassero che la clausola fosse stata effettivamente letta e compresa[31].

La Corte evidenzia poi come la clausola di prestazione del consenso non fosse stata presentata in una forma che la distinguesse chiaramente dalle altre clausole contrattua-

abusive.

27 Sentenza *Orange România*, cit., § 39; Linee Guida dell'EDPB, cit., 14-15.

28 Sentenza *Orange România*, cit., § 41.

29 Sui fattori che possono influire sulla libertà del consenso v. Linee guida dell'EDPB, cit., 8-14.

30 Sentenza *Orange România*, cit., § 45.

31 Conclusioni dell'Avvocato generale, cit., § 45; sentenza *Orange România*, cit., § 46.

li[32], rendendo quindi incerta la specificità e trasparenza del consenso richiesto. La clausola, inoltre, si limitava ad indicare, senza alcun'altra menzione, che le copie delle carte d'identità erano conservate a scopo d'identificazione[33]. Non chiariva in alcun modo al cliente che la mancata accettazione alla raccolta e conservazione del documento non fosse condizione imprescindibile alla conclusione del contratto, privandolo di fatto di un'informazione essenziale alla libera scelta[34].

Sempre sulla libertà del consenso, la Corte richiama le parole dell'Avvocato generale a sottolineare come il carattere libero fosse messo in discussione da un'ulteriore circostanza. Nell'ipotesi di un rifiuto, infatti, l'Orange România esigeva che il cliente dichiarasse per iscritto di non acconsentire né alla raccolta, né alla conservazione della copia del suo documento di identità. Tale articolata procedura, che si poneva in contrasto con la procedura lineare di conclusione del contratto, avrebbe quindi potuto indurre il cliente a ritenere la negazione del consenso non conforme alle normali regole procedurali, convincendolo erroneamente a fornirlo[35]. Il compimento da parte dell'interessato di un'azione positiva si riferisce infatti all'inequivocabilità della prestazione del consenso, non invece della sua negazione[36]. Proprio sul tema, nella sentenza *Planet49*, la Corte aveva concluso che rimuovere un segno da una casella di spunta preselezionata su un sito Internet imponesse al cliente un'azione troppo gravosa per negare il proprio consenso. Analogamente, e anzi a maggior ragione, deve quindi ritenersi eccessivamente gravosa la richiesta rivolta al cliente di negare il proprio consenso mediante l'inclusione di un'annotazione a mano[37].

A valle delle sue valutazioni e dei dubbi sollevati circa l'idoneità del consenso richiesto di soddisfare le caratteristiche sopra richiamate, la Corte lascia al giudice del rinvio il compito di valutare il caso concreto, sulla base degli ulteriori elementi fattuali in suo possesso. Tuttavia, in maniera tutt'altro che sorprendente viste le rigorose e chiare disposizioni del Regolamento, la Corte dichiara in via interpretativa generale l'inidoneità di una clausola secondo cui l'interessato sia stato informato e abbia acconsentito alla raccolta e alla conservazione di propri dati a soddisfare i requisiti del consenso privacy, nel caso in cui (i) la casella relativa a tale clausola sia stata selezionata dal titolare del trattamento dei dati prima della sottoscrizione del contratto; (ii) la clausola possa indurre in errore la persona interessata circa la possibilità di stipulare il contratto in questione anche se essa rifiuta di acconsentire al trattamento dei suoi dati; (iii) la libera scelta di opporsi sia indebitamente pregiudicata da detto titolare che richiede alla persona interessata la compilazione di un modulo supplementare per attestare il proprio rifiuto.

Tratto distintivo della sentenza in esame è forse l'espresso richiamo che fa Corte alla regola dell'onere probatorio in materia di consenso. Mentre nella sentenza *Planet49* i giudici si soffermano esclusivamente sulle condizioni di validità del consenso, in più punti della sentenza *Orange România* la Corte ribadisce l'onere in capo alla società, in

[32] Sentenza *Orange România*, cit., § 47.

[33] Ivi, § 48.

[34] Conclusioni dell'Avvocato generale, cit., § 61, sentenza *Orange România,* cit., § 49.

[35] Conclusioni dell'Avvocato generale, cit., § 60.

[36] *Ibid.*; sentenza *Orange România*, cit., § 51.

[37] Conclusioni dell'Avvocato generale, cit., § 60

qualità di titolare del trattamento, di provare che i clienti abbiano manifestato il loro consenso al trattamento dei dati personali. Prova che nel caso di specie non sembra essere stata soddisfatta. In perfetta coerenza con il principio di *accountability* – o "responsabilizzazione" – sul quale prende forma l'intero Regolamento, spetta infatti al titolare del trattamento dimostrare di aver ottenuto un valido consenso dall'interessato. Tale disposizione deve interpretarsi in maniera estensiva nel senso che il titolare deve essere in grado di dimostrare non soltanto che l'interessato ha prestato il proprio consenso, ma anche che siano state soddisfatte tutte le condizioni di efficacia[38]. La Corte puntualizza quindi come il provider non possa invertire l'onere probatorio aggravando la posizione del cliente e pretendendo che sia questo a dover manifestare attivamente il proprio rifiuto[39]. Tuttavia, come segnalato, la Corte rimette al giudice del rinvio la decisione del caso concreto.

## 5 Conclusioni e spunti di riflessione

Il consenso quale espressione di una libera volontà individuale rappresenta – quantomeno in prospettiva teorica – un potente strumento di controllo e partecipazione del singolo nella gestione delle proprie informazioni. Per adempiere a tale funzione, il consenso deve necessariamente soddisfare una stringente serie di requisiti, ora espressamente contemplati dal Regolamento e ulteriormente ribaditi dalla Corte di giustizia nelle sentenze *Planet49* e *Orange România.*

Gli interventi della Corte in materia di consenso non sono particolarmente innovativi. D'altra parte il dettagliato testo del Regolamento non lascia molto margine all'interpretazione. Le sentenze rimangono apprezzabili per riportare l'attenzione e accrescere l'*awareness* sociale sugli standard elevati richiesti dalla normativa per adoperare tale base giuridica. Tuttavia, se collocate nel più ampio dibattito dottrinale e sociale in tema di consenso privacy, le sentenze appaiono limitate. Nell'attuale scenario tecnologico, in cui raccolta, condivisone e utilizzo di informazioni sono fenomeni inarrestabili ed esponenziali, in cui le catene di titolari diventano sempre più complesse, la consapevolezza degli individui diminuisce e i trattamenti hanno impatti sull'intera collettività, la domanda non è più "come", ma "se" il consenso sia uno strumento idoneo a realizzare la funzione di controllo che gli viene affidata. La vera questione muove ormai oltre i requisiti del consenso per mettere in discussione l'efficacia del meccanismo consensuale stesso. Numerosi sono gli studi comportamentali e interdisciplinari che, analizzando la condotta degli utenti al momento della prestazione del consenso privacy, evidenziano la fragilità di tale strumento[40]. Esistono infatti una serie di fattori esogeni che, indipen-

[38] Ivi, § 49. Benché la direttiva 95/46/CE non includesse la regola dell'onere della prova in capo alle parti, secondo l'Avvocato generale la situazione giuridica non era a tal riguardo diversa. La regola si poteva infatti già evincere, almeno indirettamente, dalla previsione di cui all'art. 7 della Direttiva secondo cui la persona interessata ha manifestato il proprio consenso «in maniera inequivocabile».

[39] Sentenza *Orange România*, cit., § 51.

[40] Si veda per esempio A. Acquisti – J. Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, in A. Acquisti – J. Grossklags (a cura di) *Digital Privacy: Theory, Technologies and Practices*, New York-London, 2008; D.J. Solove, *Privacy self-management and the Consent Dilemma*, in *Harv. Law Rev.*, 126, 2013, 1880 ss.;

dentemente dal formale rispetto dei requisiti normativi, finiscono per svuotare il consenso della sua funzione di controllo riducendolo a una mera formalità, una "firma in più su un modulo prestampato"[41]. La natura astratta delle informazioni, l'impalpabilità delle conseguenze negative dei trattamenti ma anche il carattere ormai routinario dei consensi portano l'individuo a compiere scelte miopi, frettolose e irrazionali, lontane dall'espressione di un'autodeterminazione informata[42].

E alla precedente domanda, ne segue presto un'altra. Nella ormai complessa realtà della circolazione dei dati, il fallimento del consenso e di altri meccanismi di controllo individuale da un lato, e la portata ormai collettiva delle conseguenze scaturenti dai trattamenti dall'altro, portano a domandarsi se la protezione dei dati debba guardare oltre alla dimensione privata, verso una dimensione sociale e collettiva[43]. Il centro di interesse non è più la persona, considerata singolarmente e nella sua individualità, ma la persona nella collettività, quindi come raggruppamento, associazione, classe di persone accomunate da medesime caratteristiche, gusti, passioni, propensioni. I nuovi trattamenti basati su profilazione, aggregazione, classificazione, predizione hanno impatti sul singolo ma in quanto parte di una comunità. Con la seconda domanda ci si domanda quindi se sia il momento di abbandonare l'illusione di un controllo granulare del singolo, rivolgendosi a meccanismi di tutela sostanziale che proteggano la collettività dagli utilizzi pregiudizievoli e il più delle dei dati nel loro complesso.

Non sembra più sufficiente quindi che la raccolta del consenso rispetti le condizioni previste dal Regolamento. È necessaria una riflessione più profonda che rivalutando il ruolo del consenso nella disciplina sul trattamento dei dati personali porti a ridefinire l'ambito di tutela, e forse anche la natura, del diritto alla protezione dei dati personali.

F.Z. Borgesius, *Informed consent: We Can Do Better to Defend Privacy*, in *IEE*, 2015, 103; A. Chilton-O. Ben-Shahar, *Simplification of Privacy Disclosure: An Experimental Test*, in *Journ. Legal Studies*, 45, 2015, 41 ss.; L. Gatt-R. Montanari-I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in D. Poletti-P. Passagna (a cura di), *Nodi virtuali, legami informali, Internet alla ricerca delle regole*, Pisa, 2017, 57 ss.

41 Così lo definisce A. Mantelero in *Il costo della privacy tra valore della persona e ragione d'impresa,* Milano, 2007, 304, v. anche S. Patti, *Il consenso dell'interessato al trattamento dei dati personali,* in *Riv. dir. civ.*, 1999, 476 che definisce la prestazione di consenso una "vuota cerimonia".

42 V. anche I. A. Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Oss. Dir. Civ.*, 1, 2018, 67 ss.

43 A. Mantelero, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection,* in *Law & Security Review*, 32(2), 2016, 238 ss.