# CONSENSO AL TRATTAMENTO E LICEITA'

**Di Salvatore Orlando**



**SOMMARIO**: ***1. L'attualità del dibattito sul consenso privacy e sui suoi requisiti di libertà e consapevolezza. – 2. L'illiceità del trattamento dei dati personali per mancanza della base del consenso privacy in difetto di uno dei suoi requisiti di libertà, consapevolezza e manifestazione. – 3. La necessità di un dibattito sul requisito di liceità del consenso privacy. – 4. L'illiceità del trattamento dei dati personali per mancanza della base del consenso privacy in difetto del suo requisito di liceità laddove il consenso sia prestato per specifiche finalità di trattamento illegittime o il trattamento sia altrimenti vietato alla stregua di norme imperative del diritto unitario o nazionale (consenso illecito). – 5. Esempi - 5.1 Primo esempio: il consenso privacy esplicito illecito ex art. 9(2)(a) GDPR - 5.2 Secondo esempio: il divieto dell'art. 26(3) DSA. – 5.3 Terzo esempio: il divieto dell'art. 18(1)(c) del regolamento sul targeting della pubblicità politica. – 5.4 Quarto esempio: i divieti dell'art. 7 della direttiva sui lavoratori delle piattaforme online. – 5.5 Quinto esempio: i divieti di uso di sistemi di IA dell'art. 5 AI Act. – 5.6 Sesto esempio: lo sfruttamento delle vulnerabilità del Sig. Leon. – 5.7 Settimo esempio: la piattaforma illegale di concorsi a premi. – 5.8 Ottavo esempio: i divieti di trattamento della legge sull'oblio oncologico. – 5.9 Et cetera. – 6. L'invalidità del consenso privacy per illiceità è idonea a tutelare sia l'interessato che soggetti terzi. – 7. Tre aree di approfondimento. – 7.1 La finestra con vista fuori del GDPR (il test di legittimità delle finalità di trattamento non è solo endoregolamentare). – 7.2 La questione della distribuzione di competenze tra autorità amministrative e giurisdizionali in relazione all'accertamento della legittimità/illegittimità delle finalità del trattamento. – 7.3 La ricerca della cassetta degli attrezzi più adeguata per affrontare le sfide ermeneutiche del consenso privacy nella data economy. – 8. Critica esemplare al Considerando 40 della direttiva sui lavoratori delle piattaforme online a dimostrazione della necessità di dismettere la concezione che si incentra esclusivamente sui requisiti di libertà e consapevolezza del consenso privacy. – 9. Critica esemplare alla formula definitoria del diritto all'oblio oncologico nella legge 193/2023 a dimostrazione della necessità di evidenziare la figura logica del divieto che caratterizza il contemporaneo diritto dei dati. – 10. Conclusioni sul consenso privacy come atto di autonomia privata e sulla prospettiva di una nuova stagione di studi sull'atto di autonomia privata di diritto unitario sollecitata dallo studio dell'illiceità del consenso privacy.***

*ABSTRACT. È generalmente riconosciuto che il consenso privacy è invalido, e cioè non può costituire una valida base per il lecito trattamento di dati personali, in difetto di uno dei suoi requisiti di libertà, consapevolezza o manifestazione fissati espressamente dal GDPR. In questo saggio, l'a. configura un ulteriore requisito di validità del consenso privacy, quello della 'liceità', argomentando che esso consiste nel requisito per cui le specifiche finalità di trattamento dei dati personali per le quali il consenso privacy è prestato devono essere legittime e il trattamento non deve essere altrimenti vietato alla stregua di norme imperative del diritto unitario o del diritto nazionale applicabile. L'a. offre numerosi esempi di consenso privacy*



ISSN 2239-8570

*che, a suo avviso, deve ritenersi tipicamente illecito (per difetto del requisito di liceità) e dunque invalido, pur essendo stato in ipotesi reso dall'interessato in modo libero e consapevole, ed espresso in modo specifico ed inequivocabile, o anche, se richiesto dalla legge, esplicito. Il saggio si sofferma dunque sui problemi ermeneutici collegati all'applicazione del requisito di liceità del consenso privacy, individuando alcune aree di approfondimento. In particolare, l'a. evidenzia le esigenze di coordinamento tra il GDPR e le altri fonti di diritto unitario e nazionale alla stregua delle quali va asseverata la liceità, nonché le esigenze di coordinamento e di cooperazione tra le varie autorità amministrative e giurisdizionali che possono essere di volta in volta coinvolte in relazione al medesimo giudizio. Infine, l'a. argomenta in favore della tesi per la quale il consenso privacy debba essere concepito quale atto di autonomia privata, e spiega perché, a suo avviso, le categorie del divieto e dell'illiceità, con le quali il giurista europeo è tenuto a cimentarsi interpretando il GDPR e le altre fonti dell'erigendo diritto europeo dei dati che fissano limiti all'industria dei dati, costituiscano le categorie dalle quali partire per una nuova stagione di studi sul diritto europeo dell'autonomia privata.*

*It is commonly recognised that privacy consent shall be deemed invalid, i.e. it may not constitute a basis for lawful processing of personal data, lacking one of its requirements of freedom, awareness and disclosure, as provided for by the GDPR. In this essay, the a. identifies 'lawfulness' as a further requirement of privacy consent, arguing that it consists in the requirement that the specific purposes for the personal data processing for which the privacy consent is given shall be legitimate and the processing shall not be otherwise prohibited, in each case on the basis of the operation of mandatory provisions of Union or national law, as applicable. The essay illustrates a number of cases where privacy consent shall be deemed illegal (for lack of the lawfulness requirement) and therefore invalid, although being given freely and in a specific, informed and unambiguous manner by the data subject. The essay further illustrates some problems of interpretation deriving from the application of the lawfulness requirement of the privacy consent. In particular, the a. identifies some issues relating to the coordination between GDPR and the other sources of Union and national law on the basis of which the test to establish whether the processing purposes are legitimate shall be carried out. The a. further underlines the existence of problems of coordination and the need for cooperation between and among the various administrative and judicial authorities that may be involved in connection with the test relevant to the lawfulness requirement of the privacy consent. Finally, the a. argues in favour of the thesis for which privacy consent shall be treated in terms as an act of private autonomy and explains why, in his view, the categories of 'prohibition' and 'unlawfulness' that the European jurists shall deal with in interpreting the GDPR and the other provisions of the rising EU data law setting limits to the data industry, will constitute a useful subject for a new season of legal studies in private autonomy theory as a matter of EU law.*



ISSN 2239-8570

## 1. L'attualità del dibattito sul consenso privacy e sui suoi requisiti di libertà e consapevolezza.

La discussione sul consenso al trattamento dei dati personali (di seguito per brevità anche "consenso privacy") come base per il trattamento lecito dei dati personali ai sensi dell'art. 6(1)(a) del Regolamento (UE) 2016/679 (di seguito anche "GDPR" o il "Regolamento")[1] è tornata di grande attualità dopo le numerose decisioni adottate dallo *European Data Protection Board* (di seguito anche "EDPB") e dalla Corte di giustizia dell'Unione europea (di seguito anche "CGUE") in relazione a importanti tipologie di trattamenti di dati personali effettuati da società del gruppo Meta, con le quali, in sintesi, è stata ripetutamente negata la possibilità di utilizzare tanto la base dell'esecuzione del contratto quanto quella del legittimo interesse per i servizi Facebook, Instagram e WhatsApp[2], con ciò, sostanzialmente, indican-

[1] Art. 6(1)(a) GDPR: "1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; […]".

[2] Si fa riferimento innanzitutto alle tre decisioni vincolanti dello EDPB del 5 dicembre 2022 e ai successivi provvedimenti dell'autorità di controllo irlandese nei confronti di Meta del successivo 31 dicembre 2022 (per i servizi FB e Instagram) e di WhatsApp del gennaio del 2023, che hanno impedito a queste piattaforme di continuare ad utilizzare la base dell'esecuzione del contratto.
Successivamente, nell'ambito della controversia tra *Meta Platforms Inc*. e il *Bundeskartellamt* (l'autorità federale garante della concorrenza della Repubblica Federale di Germania) con sentenza del 4 luglio 2023, la CGUE ha dichiarato che l'articolo 6(1)(b) GDPR - che prevede la base giuridica dell'esecuzione di un contratto - debba essere interpretato nel senso che il trattamento di dati personali effettuato da Meta a proposito di Facebook, consistente nella profilazione a fini pubblicitari dell'utente, può essere considerato necessario per l'esecuzione di un contratto del quale gli interessati sono parti solo a condizione che detto trattamento sia oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata a quegli stessi utenti, cosicché l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento. In quella sentenza, la CGUE ulteriormente negato di per sé rilevanza al fatto che un simile trattamento dei dati personali sia menzionato nel contratto oppure che esso sia soltanto utile per la sua esecuzione. In particolare, secondo quanto si trova dichiarato dalla CGUE in quella sentenza, l'elemento determinante ai fini dell'applicazione della base giuridica del contratto è che il trattamento sia essenziale per consentire la corretta esecuzione del contratto stipulato tra quest'ultimo e l'interessato e che, pertanto, non esistano altre soluzioni percorribili e meno invasive. Quanto alla base giuridica del legittimo interesse, la CGUE dichiarava (sempre in quella sentenza) che la base prevista dall'articolo 6(1)(f) GDPR può essere considerata idonea per la pubblicità profilata solo se: *(i)* il titolare del trattamento abbia precisamente informato gli interessati in merito al legittimo interesse; *(ii)* tale trattamento sia effettuato entro i limiti di quanto strettamente necessario alla realizzazione di suddetto interesse; e *(iii)* il contemperamento delle contrapposte pretese non comporti una prevalenza delle libertà e dei diritti fondamentali di tali utenti che richiedano la protezione dei dati personali sul legittimo interesse del titolare. Riferendosi al caso concreto che formava oggetto dei quesiti rivoltile in quel giudizio, la CGUE concludeva dichiarando che, in conseguenza di quanto sopra, né il contratto, né il legittimo interesse (né tantomeno l'obbligo legale o l'interesse vitale) potessero essere considerati basi giuridiche idonee ai fini della pubblicità personalizzata operata da Meta.
Ed infine il 27 ottobre 2023 l'EDPB ha emesso una decisione vincolante e urgente, la n. 01/2023, affinché l'autorità di controllo irlandese vieti definitivamente a Meta Ireland Limited di trattare i dati personali dei propri utenti per fini di pubblicità comportamentale sia sulla base del contratto che su quella del legittimo interesse: https://edpb.europa.eu/our-



ISSN 2239-8570

dosi la necessità di ricorrere alla base del consenso; nonché dopo le prime contestazioni sulla liceità del trattamento di dati personali mosse ad OpenAI ai sensi del GDPR in relazione al servizio ChatGPT[3], e ai dubbi suscitati dalla spiegazione fornita dalla medesima società di ricorrere alla base del legittimo interesse per il trattamento di dati personali, da cui il recente rapporto della *task force* costituita *ad hoc* in seno all'EDPB per valutare la questione[4].

Di grande attualità è in particolare il tema dei requisiti del consenso privacy, *in primis* quelli che attengono alla consapevolezza e alla libertà dell'interessato, che, come risaputo, devono ricorrere per la prestazione di un consenso valido, ai sensi dell'art. 4, n. 11) del Regolamento[5].

Tale tema, già centrale nel dibattito sul c.d. *tying*[6], ha ricevuto di recente un nuovo impulso a proposito della diffusione delle formule c.d. *Pay or Ok*

work-tools/our-documents/urgent-binding-decision-board-art-66/urgent-binding-decision-012023_en.

[3] Ci riferiamo innanzitutto al provvedimento cautelare della nostra Autorità garante per la protezione dei dati personali (di seguito anche il "Garante privacy italiano") del 30 marzo 2023, alla successiva misura di sospensione condizionata del medesimo provvedimento dell'11 aprile 2023 e all'atto di contestazione di violazione della normativa in materia di protezione dei dati personali relativamente al servizio ChatGPT che il Garante privacy italiano ha notificato a OpenAI LLC e ha comunicato al pubblico il 29 gennaio 2024. Nel comunicato, il Garante specificava che la misura segue il provvedimento adottato dalla medesima Autorità il 30 marzo 2023, e che l'istruttoria svolta ha fatto emergere elementi che possono configurare una o più violazioni delle disposizioni del GDPR (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020).

[4] Il report del 23 maggio 2024 evidenzia una serie di criticità del servizio ChatGPT circa il rispetto delle prescrizioni del GDPR, toccando i temi della liceità del trattamento (in particolare sottolineando la necessità che ricorra una delle basi previste dal primo paragrafo dell'art. 6 del Regolamento e prendendo in considerazione le diverse fasi e attività implicate dal servizio, quali la raccolta, compreso il *web scraping*, la preelaborazione e l'addestramento dei dati, nonché le attività e fasi di *input*, *prompt* e *output*) della correttezza, della trasparenza e degli obblighi di informazione, dell'accuratezza e dei diritti degli interessati (https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf).

[5] Art. 4, n. 11) GDPR «'consenso dell'interessato': 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».

[6] Espressione con la quale si fa riferimento all'eventualità, considerata nell'art. 7(4) GDPR, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto. I Considerando 42 e 43 del GDPR chiaramente collegano questa disposizione al requisito di libertà del consenso privacy. Limitandoci ad alcuni dei contributi più recenti (ai quali si rinvia anche per riferimenti più completi alla dottrina precedente e alla giurisprudenza rilevante) cfr.: P. STANZIONE, *La libertà e il suo valore*, in *Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione*, a cura di G. Cerrina Feroni, Il Mulino, Bologna, 2024, 149 ss.; G. FINOCCHIARO, *Consenso al trattamento e libertà*, in *Pers. merc.*, 2024, 3 ss.; V. RICCIUTO, *Consenso al trattamento e contratto*, in *Pers. merc.*, 2024, 14 ss., spec. 22 ss.; ID., *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022; G. SCORZA, *La deducibilità nell'oggetto del contratto del diritto a trattare i dati personali*, in *Commerciabilità dei dati personali*, cit., 231 ss. spec. 245 ss.; C.A. TROVATO, Everything has its price? *Una riflessione sulle pratiche di commercializzazione dei dati* personali, ivi, 301 s.; E. TOSI, *Dati personali e contratto: un ossimoro apparente*, in *European Journal of Privacy Law & Technologies*, 2023/2, 79 ss.;



ISSN 2239-8570

(note anche come "*Consent or Pay*", o "acconsenti o paga"). Esse, implementate a partire dal 2022 da alcune testate giornalistiche online[7], si sono recentemente diffuse presso Facebook e altre piattaforme, che hanno inteso così adeguarsi all'indicazione circa la doverosità della base del consenso, espressa nei predetti provvedimenti riguardanti i servizi di Meta.



ID., *Circolazione contrattuale dei dati personali tra contratto e responsabilità,* Milano, 2023; F.A. GENOVESE, *Trattamento dei dati personali e consenso dell'interessato*, in *La circolazione dei dati personali: persona, contratto e mercato*, a cura di A. Morace Pinelli, Pisa, 2023, 93 ss.; A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in *Riv., trim. dir. proc. civ.*, 2022, 711 ss.; S. ORLANDO, *Il coordinamento tra la direttiva 2019/770 e il GDPR. L'interessato-consumatore*, in *Pers. merc.*, 2023, 230 ss., e in *Commerciabilità dei dati personali*, cit., 157 ss.; ID., *Per un sindacato di liceità del consenso privacy*, in *Pers. merc.*, 2022, 528 ss.; F. CAGGIA, *Cessione di dati personali per accedere al servizio digitale gratuito: il modello del "consenso rafforzato"*, in *I problemi dell'informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro*, Roma, 2022, 417 ss; L. CASALINI, *Dati e identità personale. Note sparse a partire da una recente pronuncia del Consiglio di Stato*, in *Annuario 2022 Osservatorio Giuridico sull'Innovazione Digitale*, a cura di S. Orlando e G. Capaldo, Roma, SUE, 2022, 53 ss.; A. DE FRANCESCHI, *Personal data as Counter-Performance*, in *Privacy and Data Protection in Software Services*, a cura di R. Senigaglia, C. Irti e A. Bernes, Singapore, Springer, 2022, 59 ss.; ID, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, 67 ss.; P. HACKER, *Regulating the economic impact of data as counter-performance: from the illegality doctrine to the unfair contract terms directive*, in *Data as counter-performance – Contract law 2.0?* a cura di S. Lohsse, R. Schulze e D. Staudenmayer, Bloomsbury Publishing, Londra, 2020, 47 ss.; V. JANEˇCEK, G. MALGIERI, *Data extra commercium*, ivi, 95 ss.; S. LOHSSE, R. SCHULZE, D. STAUDENMAYER, *Data as counterperformance – contract law 2.0? An introduction*¸ ivi, 9 ss.; A. METZGER, *A market model for personal data: state of play under the new directive on digital content and digital services*, ivi. cit., 25 ss.; S. VAN ERP, *Management as ownership of data*, ivi, 77 ss.; C. WENDEHORST, *Personal data in data value chains – is data protection law fit for the data economy?,* ivi, 193 ss.; C. SOLINAS, *Autonomia privata e regolazione pubblica nel trattamento dei dati personali*, Bari, 2022; A.M. GAMBINO e A. STAZI, *Introduzione. Datificazione dei rapporti socio-economici, circolazione dei dati e diritto*, in *La circolazione dei dati*, a cura di A.M. Gambino e A. Stazi, Pisa, Pacini, 2020, XI; G. MARCHETTI e S. THOBANI, *La tutela contrattuale dei consumatori di contenuti e servizi digitali*, in *Manuale di diritto privato delle nuove tecnologie* a cura di G. Magri, S. Martinelli e S. Thobani, Torino, Giappichelli, 2022, 35 ss. spec. 46 ss.; G. D'IPPOLITO, *Monetizzazione, patrimonializzazione e trattamento dei dati personali*, in *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, a cura di E. Cremona, F. Laviola, V. Pagnanelli, Torino, Giappichelli, 2022, 51 ss. Per i problemi generali interessati dalla tematica della libertà del consenso nell'ecosistema digitale, cfr. anche i contributi di C. CAMARDI, *Dalla logica individualistica alla regolazione della complessità nella tutela del consumatore (e delle vulnerabilità) nell'ecosistema digitale*, in *Mercato digitale e tutela dei consumatori. Prove di futuro*, a cura di G. Grisi e S. Tommasi, Torino, 2023, 217 ss.; A. MORACE PINELLI, *Introduzione*, in *La circolazione dei dati personali: persona, contratto e mercato*, cit. 11 ss.

[7] V. i comunicati del Garante privacy italiano del 18.10.2022 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9815415), del 21.10.2022 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9816536) e del 12.11.2022 (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9822601) di avvio di istruttorie a carico di testate editoriali online. In dottrina, cfr. R. MONTINARO, *I* cookie paywall *e le testate giornalistiche* online*: si tratta di un "consenti a tutto o paga"?*, in *Mercato digitale e tutela dei consumatori*, cit., 187 ss.



ISSN 2239-8570

Sul punto - alimentando ulteriormente il dibattito - è intervenuto da ultimo il parere dell'EDPB 8/2024[8]. In esso, l'EDPB ha esaminato la compatibilità della formula acconsenti o paga con il requisito di libertà del consenso, limitatamente, tuttavia, alle "piattaforme online di grandi dimensioni", una categoria - dobbiamo sottolinearlo - disegnata *ad hoc* dall'EDPB ai fini del medesimo parere, e che non ha un riscontro normativo. Facendo ciò, l'EDPB ha dichiaratamente escluso dal suo parere i trattamenti di dati personali operati da titolari diversi dalle "piattaforme online di grandi dimensioni", tra cui anche - così sembra doversi ritenere - le testate giornalistiche online che hanno per prime diffuso la formula *Pay or Ok*.

Nell'ambito tematico dei requisiti di consapevolezza e libertà del consenso privacy deve inquadrarsi anche la crescente attenzione riservata al *consenso al trattamento dei dati personali ottenuto in modo sleale, ossia falsato da comportamenti scorretti sulle interfacce online*. È il fenomeno noto con l'espressione "*dark patterns*", più di recente sostituita da quella "*deceptive design patterns"*[9].

Con queste espressioni si individuano certe caratteristiche fuorvianti delle interfacce online, ossia dei software che governano l'esperienza degli utenti online[10]. Il fenomeno riguarda il disegno di questi software, che può essere piegato a fini di distorsione del comportamento degli utenti online. Esso non riguarda, dunque, soltanto la distorsione del consenso privacy, concernendo qualsiasi comportamento dell'utente online. Naturalmente, però, poiché questo fenomeno investe anche e massicciamente l'influenza sulla prestazione del consenso privacy, di esso si è interessato l'EDPB, che ha emanato delle apposite Linee guida (la prima versione era intitolata *ai dark patterns*; quella più recente del febbraio 2023, la versione 2.0, è intitolata ai *deceptive design patterns*, ossia, come detto, la nuova espressione per indicare lo stesso fenomeno)[11]; e il Garante privacy italiano ha pubblicato sul suo sito internet una pagina informativa[12].

A questo fenomeno sono dedicati segnatamente il Considerando 67 e l'art. 25 del *Digital Services Act* (il regolamento (UE) 2022/2065, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE, innanzi anche "DSA").

Il tema si intreccia con quello della disciplina delle pratiche commerciali scorrette, di cui alla direttiva 2005/29/CE (innanzi anche "UCPD"), renden-

[8] Parere 8/2024 dell'EDPB del 17 aprile 2024: https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf

[9] Cfr. S. ORLANDO, *A proposito dei deceptive design (già dark) patterns*, in *Mercato digitale e tutela dei consumatori*, cit. 63 ss.

[10] La definizione di interfaccia online è contenuta all'art. 3 lett. *m)* del DSA: "«interfaccia online»: qualsiasi software, compresi i siti web o parti di essi, e le applicazioni, incluse le applicazioni mobili".

[11] https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[12] https://www.garanteprivacy.it/temi/internet-e-nuove-tecnologie/dark-pattern



ISSN 2239-8570

do necessario instaurare ermeneuticamente il giusto rapporto tra questi tre plessi normativi (UCPD, GDPR e DSA)[13].

Infine, e naturalmente, nel dibattito sul ruolo del consenso privacy come base del trattamento dei dati personali, risulta centrale - e, per essere franchi: ancora tutta da centrare - l'analisi delle recenti e numerose normative che hanno contrattualizzato o preso atto della contrattualizzazione[14] di una pluralità di rapporti che comportano la disposizione e il trattamento di dati personali su base volontaria.

Si fa riferimento alla *Digital Content Directive* (di seguito anche "DCD")[15], alla direttiva *Omnibus*[16], al *Data Governance Act* (di seguito anche "DGA")[17], al DSA[18], al *Data Act*[19].

---

[13] Non possiamo soffermarci qui su questo aspetto, che richiederebbe una trattazione *ad hoc*. Per un primo orientamento, v. S. ORLANDO, *A proposito dei deceptive design (già dark) patterns*, cit. spec. 98 ss. e 106 s. Il tema del rapporto tra fonti nel diritto dei dati non si esaurisce, naturalmente, all'ambito delle fonti che rispondono al principio del divieto dello sfruttamento delle vulnerabilità decisionali delle persone fisiche (di cui è espressione la disciplina di contrasto dei c.d. *deceptive design patterns*), ma investe ogni altro ambito del diritto dei dati nel quale possano ravvisarsi principî comuni a più fonti. Per fare un esempio, è questo l'ambito del contrasto alla discriminazione, dove pure si pongono problemi di coordinamento tra varie fonti del diritto dei dati (cfr. per tutti, S. TOMMASI, *The Risk of Discrimination in the Digital Market. From the Digital Services Act to the Future,* Springer, 2023).

[14] Come noto, il dibattito sulla contrattualizzazione dei rapporti che comportano il trattamento dei dati personali è molto acceso. Per un'analisi ragionata ed aggiornata delle diverse posizioni, ed i relativi riferimenti bibliografici, v. per tutti V. RICCIUTO, *Consenso al trattamento e contratto*, cit. 14 ss.

[15] Direttiva (UE) 2019/770 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali. Viene in particolare in rilievo la seguente proposizione dell'art. 3(1) DCD: «[…] La presente direttiva si applica altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore *e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico*, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti».

[16] Direttiva (UE) 2019/2161 (UE) 2019/2161 che modifica la direttiva 93/13/CEE e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori. In particolare, viene in rilievo l'art. dall'art. 4, punto 2), lett. b) della direttiva *Omnibus*, che ha inserito l'art. 1-*bis* nella direttiva 2011/83/UE contenente una disposizione conforme a quella sopra riportata dell'art. 3(1) DCD: «1-*bis*. La presente direttiva si applica anche se il professionista fornisce o si impegna a fornire un contenuto digitale mediante un supporto non materiale o un servizio digitale al consumatore *e il consumatore fornisce o si impegna a fornire dati personali al professionista*, tranne i casi in cui i dati personali forniti dal consumatore siano trattati dal professionista esclusivamente ai fini della fornitura del contenuto digitale su supporto non materiale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui il professionista è soggetto, e questi non tratti tali dati per nessun altro scopo».

[17] Regolamento (UE) 2022/868 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724. Del DGA vengono in rilievo la disciplina sull' «intermediazione dei dati» (Capo III artt. 10-15 DGA) e quella sull'«altruismo dei dati» (Capo IV, artt. 16-25 DGA), che riguardano entrambe tanto dati non personali che dati personali e che prevedono chiaramente titoli e rapporti contrattuali per la condivisione dei dati, come ivi prevista e definita. Il servizio di intermediazione di dati è definito come quel servizio che mira



ISSN 2239-8570

Mentre in tutte queste fonti è dichiarata e ribadita la prevalenza del GDPR, risulta ancora mancante in dottrina, presso i giuristi europei, un disegno teorico organico idoneo a legare tutte queste normative in una trama concettuale unitaria, coerente e sufficientemente condivisa, che vada al di là della, pacifica, dichiarazione della prevalenza del GDPR. In questo contesto, e nel difetto di una teoria unitaria, quella dichiarazione rischia effettivamente di diventare una formula declamatoria vuota o imperfetta; inidonea, cioè, ad orientare efficacemente l'interpretazione e l'applicazione delle norme nella ricerca di soluzione ai molti problemi applicativi che già si intravedono.

## 2. L'illiceità del trattamento dei dati personali per mancanza della base del consenso privacy in difetto di uno dei suoi requisiti di libertà, consapevolezza e manifestazione

Come noto, al principio di liceità del trattamento dei dati personali, enunciato all'art. 5(1)(a) del Regolamento[20], secondo cui i dati personali devono essere trattati in modo lecito (oltre che corretto e trasparente nei confronti dell'interessato), segue la disposizione del paragrafo 1 dell'art. 6 GDPR, a tenore del quale il trattamento è lecito solo se e nella misura in cui ricorra

a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, *rapporti commerciali ai fini della condivisione dei dati* tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali (art. 2, n. 11 DGA). Ai fini di questa definizione e di quella sull'altruismo dei dati, il DGA definisce la «condivisione dei dati» come la fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, *sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario, ad esempio nel quadro di licenze aperte o commerciali, dietro compenso o a titolo gratuito* (art. 2, n. 10 DGA). L'altruismo dei dati è definito come la condivisione volontaria di dati sulla base del *consenso accordato dagli interessati al trattamento dei dati personali* che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, *senza la richiesta o la ricezione di un compenso* che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale (art. 2, n. 16 DGA).

[18] Del DSA vengono in rilievo le norme che prevedono che i destinatari dei servizi di piattaforme online possano modificare i parametri della pubblicità ad essi rivolta (art. 26 DSA) e le opzioni che influenzano i parametri dei sistemi di raccomandazione che determinano l'ordine delle informazioni ad essi presentate (art. 27 DSA).

[19] Regolamento (UE) 2023/2854 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828. Del *Data Act* vengono in rilievo la disciplina della condivisione su base contrattuale dei dati da impresa a consumatore e da impresa a impresa, compresa la condivisione dei dati generati dall'uso di prodotti connessi e dei servizi correlati, come ivi definiti (Capi II e III, artt. 3-12 *Data Act*) e quella delle clausole abusive nei contratti tra imprese che hanno ad oggetto l'accesso e l'utilizzo di dati (Capo IV, art. 13 *Data Act*).

[20] Art. 5(1)(a) GDPR: "1. I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);[…]".



ISSN 2239-8570

una delle condizioni previste nelle lettere da a) a f) del medesimo paragrafo: le cosiddette 'basi' del trattamento.

Il modo tradizionale di affrontare il problema della liceità a proposito del trattamento dei dati personali segue questa scansione normativa.

Pertanto, quando viene in questione la ricorrenza della base del consenso privacy, si dice che il trattamento dei dati personali è lecito se l'interessato abbia prestato un consenso che abbia tutti i requisiti previsti per il consenso dall'art. 4, n. 11) GDPR: una 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[21].

Sono le condizioni che in breve possiamo chiamare come requisiti di libertà, consapevolezza e manifestazione del consenso privacy.

Ogni dichiarazione dell'interessato prestata senza i prescritti requisiti di libertà, consapevolezza e manifestazione previsti dal GDPR per il consenso privacy si intende prestata «in violazione» del Regolamento, e dunque «non è vincolante» come consenso (arg. art. 7, par. 2, ultima proposizione GDPR).

Questo sta anche a significare che quando ci si riferisce alle condizioni appena richiamate di libertà, consapevolezza e manifestazione del consenso, *il loro difetto comporta l'illiceità del trattamento* dei dati personali ex art. 5(1)(a) del Regolamento, in quanto il consenso, non avendo una di quelle condizioni o requisiti, non è vincolante come tale, e dunque viene a mancare la necessaria "base" per un trattamento lecito dei dati personali.

Rivolgendoci ora alle tipologie problematiche di condizionamento del consenso privacy richiamate dianzi, che - come abbiamo detto (v. par. 1 *supra*) - occupano attualmente in misura quasi esclusiva il dibattito sul consenso privacy, ossia ai fenomeni dei *dark* o *deceptive design patterns*, del *tying*, e delle formule *Pay or Ok* , possiamo dire conclusivamente che ad essere in gioco per ciascuno di tali fenomeni sono la liceità/illiceità del *trattamento* a seconda della ricorrenza/mancanza dei requisiti di libertà e consapevolezza del *consenso* privacy.

Così, in particolare, quando il consenso privacy è falsato dalle interfacce attraverso "percorsi oscuri" o "modelli fuorvianti", sarà corretto parlare di illiceità del *trattamento* per difetto di un consenso vincolante come tale, perché il consenso ottenuto dal titolare in quel modo difetta delle condizioni di consapevolezza, e talvolta anche della condizione di libertà, prescritte dal Regolamento, e dunque non è valido e vincolante come consenso ai sensi del GDPR come base di un trattamento lecito. Allo stesso modo, le indagini sui requisiti del consenso privacy svolte a proposito del *tying* e delle formule "acconsenti o paga" riguardano le alternative, di cui dispone in concreto l'interessato, in quanto ritenute rilevanti per asseverare la sua effettiva libertà e talvolta anche la sua effettiva consapevolezza nel prestare il consenso privacy. Con la conseguenza che dovrà ritenersi il consenso privacy invalido per difetto di quei requisiti e il relativo trattamento dei dati personali illecito

[21] Cfr. *ex multis*, F.A. GENOVESE, *Trattamento dei dati personali e consenso dell'interessato*, cit. spec. p 91 ss.





ISSN 2239-8570

tutte le volte in cui le indagini condotte in concreto portino alla conclusione dell'assenza in concreto dei requisiti di libertà e/o consapevolezza.



## 3. La necessità di un dibattito sul requisito di liceità del consenso privacy

Salvo che per alcune sollecitazioni[22], non sembra invece essersi ancora sviluppato un dibattito su un requisito del consenso privacy per così dire implicito, ossia non espressamente contemplato dalla lettera del GDPR: il requisito della liceità del consenso privacy.

Intendo qui riferirmi ad un requisito *ulteriore e autonomo* rispetto a quelli di libertà, consapevolezza e manifestazione, sopra ricordati. Per chiarezza, chiamerò nel prosieguo del presente contributo il consenso privacy che difetti del requisito di liceità - nel senso specifico che proverò di seguito ad esporre - come consenso privacy *illecito*. Devo però al contempo segnalare, in proposito, che in letteratura e in alcuni provvedimenti del Garante privacy italiano, si utilizza talvolta l'espressione «consenso illecito» per far riferimento proprio al consenso privacy che difetta dei requisiti di libertà, consapevolezza e manifestazione previsti espressamente dal GDPR e ricavati dalla definizione di consenso ex art. 4, n. 11 del Regolamento[23]. Spero di riuscire ad esporre in modo convincente nel presente saggio i motivi per i quali ritengo invece corretto e utile individuare e indicare con il concetto di «illiceità» un distinto spazio di trattamento e di valutazione normativa del consenso privacy.

Il requisito di liceità del consenso privacy, inteso in questa accezione autonoma dai requisiti ricavati dall'art. 4, n. 11 GDPR, deve a mio avviso delinearsi sulla base del combinato disposto delle previsioni dell'art. 5(1)(b), nella parte in cui prescrive che i dati personali debbano essere «raccolti per finalità […] *legittime*»[24], e dell'art. 6(1)(a) GDPR. Quest'ultima disposizio-

[22] Cfr. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di R. Pardolesi, Milano, 2003, 395, spec. p 412-413 e 415; S. ORLANDO, *Per un sindacato di liceità del consenso privacy*, in *Pers. merc.* 2022, 527 ss.; D. IMBRUGLIA, *Le presunzioni delle macchine e il consenso dell'interessato*, in *Riv. trim. dir. proc. civ.*, 2023, 921 ss., spec. p 944-945; G. VETTORI, *Rodolfo Sacco e la civilistica del XXI secolo*, in *Esperienze giuridiche in dialogo. Il ruolo della comparazione*, a cura di M. Graziadei e A. Somma, Sapienza Università Editrice, Roma, 2024, 143, e in *Riv. trim. dir. proc. civ.*, 2023, 539 ss.

[23] Cfr. per tutti G. SCORZA, *La deducibilità nell'oggetto del contratto del diritto a trattare i dati personali*, cit., 245 ss. Per i provvedimenti del Garante privacy italiano, v. quello del 23 febbraio 2023 nei confronti di Ediscom S.A. nel quale si legge il seguente passaggio «In conclusione si è ritenuto che, un consenso raccolto con tali modalità, volutamente progettate per eludere le norme, destasse molte perplessità in ordine alla libertà e alla consapevolezza con cui l'interessato può esprimere la propria volontà e pertanto non poteva essere considerato lecito» (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870014).

[24] Art. 5(1)(b) GDPR: "I dati personali sono: […] b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);



ISSN 2239-8570

ne va coordinata con la prima nel senso che deve essere aggiunto in via interpretativa l'aggettivo «legittime» al sostantivo «finalità» ivi utilizzato, così che la relativa condizione dell'art. 6(1)(a) GDPR deve essere letta come se recitasse: «l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità *legittime*».

Una simile lettura non sembra possa essere messa in dubbio, essendo assolutamente pacifico che i principî di cui all'art. 5 GDPR trovino applicazione con riferimento a ciascuna e a tutte le condizioni per il trattamento lecito, di cui al successivo art. 6.

Non vedendosi d'altronde come potrebbe sostenersi che costituisca una base di lecito trattamento dei dati personali quella per cui l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità *illegittime*, deve senz'altro concludersi che l'aggettivo 'legittime' è sottinteso nella lettera a) del primo paragrafo dell'art. 6 del Regolamento.

Se si conviene con quanto sopra, si dovrà anche riconoscere – già in astratto - la possibilità che le specifiche finalità di trattamento per le quale il titolare del trattamento chiede e ottiene il consenso dall'interessato, possano essere illegittime. Ed invero, come il Regolamento implicitamente prevede che esse *debbano* essere legittime, si dovrà convenire che il medesimo Regolamento implicitamente preveda che esse *possano* essere illegittime.

Ed è questo appunto il campo per il sindacato della liceità del consenso privacy, di cui sembra corretto debba affacciarsi la necessità di un dibattito. Quelle norme, in altre parole, consentono uno specifico sindacato di liceità del consenso privacy (ulteriore e diverso rispetto a quello che riguarda i requisiti di libertà, consapevolezza e manifestazione, fissati dall'art. 4, n. 11 GDPR), ma al contempo lo impongono, perché impongono di considerare l'ipotesi che le specifiche finalità del trattamento dei dati personali per cui l'interessato presta il consenso privacy siano illegittime.

Per lo stesso motivo, e in via più generale, non sembra possa negarsi nemmeno in linea teorica che debba considerarsi invalido un consenso privacy reso da un interessato a fronte di *un divieto legale posto al titolare del trattamento di raccogliere i dati personali che formano oggetto di quel consenso privacy*. Come vedremo più avanti, i divieti di questo tipo sono variamente articolati (par. 4 *infra*), e numerosi sono gli esempi che possono farsi al riguardo (par. 5 *infra*). Essi confluiscono tutti nell'ambito tematico del dibattito che sembra necessario promuovere sulla liceità del consenso privacy.

[…]". Che la determinata finalità del trattamento per la quale l'interessato acconsente al trattamento debba essere «legittima» è previsto espressamente anche nel nuovo regime dell'altruismo dei dati predisposto dal *Data Governance Act*. V. art. 21(1)(a) DGA: "1. Un'organizzazione per l'altruismo dei dati riconosciuta informa in maniera chiara e facilmente comprensibile gli interessati o i titolari dei dati, prima di qualsiasi trattamento dei loro dati, in merito: a) agli obiettivi di interesse generale e, se opportuno, alla finalità determinata, esplicita e legittima per cui i dati devono essere trattati, e per i quali acconsentono al trattamento dei loro dati da parte di un utente dei dati".



ISSN 2239-8570

### 4. L'illiceità del trattamento dei dati personali per mancanza della base del consenso privacy in difetto del suo requisito di liceità laddove il consenso sia prestato per specifiche finalità di trattamento illegittime o il trattamento sia altrimenti vietato alla stregua di norme imperative del diritto unitario o nazionale (consenso illecito).

Alla luce delle considerazioni svolte nel par. 3 *supra*, sembra corretto postulare un requisito di liceità del consenso privacy diverso dai requisiti di libertà, consapevolezza e manifestazione del consenso privacy.

Sembra ulteriormente corretto ritenere che, similmente a quanto accade per il difetto dei requisiti di libertà, consapevolezza e manifestazione del consenso privacy, debba dirsi che anche nel caso di difetto del requisito di liceità del consenso privacy (inteso nel senso detto), il trattamento dei dati personali dovrà ritenersi illecito.

Ciò in quanto, anche in questo caso, dovrà dirsi che una dichiarazione dell'interessato prestata per acconsentire al trattamento di propri dati personali per finalità *illegittime*, in contrasto con la prescrizione dell'art. 5(1)(b) GDPR, costituisce una «violazione» del Regolamento e come tale non è «vincolante» (arg. art. 7, par. 2 ultima proposizione GDPR). E cioè che essa non è vincolante come consenso privacy.

Pertanto qualsiasi dichiarazione di consenso al trattamento dei dati personali prestata per una o più specifiche finalità di trattamento illegittime non può costituire una valida base per il trattamento dei dati personali.

In questo senso, potrà sinteticamente dirsi anche che l'illiceità del consenso privacy (nello specifico senso qui esposto) comporta l'illiceità del relativo trattamento dei dati personali, ossia del trattamento dei dati personali che voglia basarsi sul consenso privacy illecito.

Se si conviene con quanto sopra, dovrà ora anche convenirsi sul fatto che la rilevanza della legittimità delle finalità del trattamento ai fini del giudizio sulla validità del consenso privacy consente ed impone di ritenere rilevanti i divieti legali di trattamento di dati personali.

Come esporrò nel successivo paragrafo dedicato agli esempi (v. par. 5 *infra*), divieti di questo tipo sono sempre più numerosi a cospetto della definitiva affermazione della *data economy*, e della conseguente esigenza, sempre più avvertita dal legislatore europeo e dai legislatori nazionali, di porre dei limiti legali all'industria dei dati.

Tali divieti si presentano come variamente articolati, prevedendo e combinando insieme in modi di volta in volta diversi (in relazione alle diverse finalità disciplinari assolte dai divieti) gli elementi rilevanti per la fattispecie del divieto, e così disegnando variamente quelli relativi ai destinatari del divieto (generalità dei titolari o determinate categorie di titolari del trattamento dei dati) ai dati personali che formano l'oggetto del trattamento vietato (generalità dei dati personali o determinate categorie di dati personali) e alle finalità del trattamento (qualsiasi finalità o determinate categorie di finalità), nonché inserendo la previsione di altre circostanze fattuali variamente qualificate, anche temporalmente.



ISSN 2239-8570

Potranno dunque definirsi invalidi in quanto illeciti, tanto i consensi privacy prestati a fronte di specifici divieti posti a determinate categorie di titolari di trattare determinate categorie di dati personali per determinate finalità (ove il consenso privacy riguardi dati personali rispondenti a quelle determinate categorie e sia prestato per quelle determinate finalità vietate), quanto i consensi privacy prestati a fronte di specifici divieti rivolti alla generalità dei titolari di trattare determinate categorie di dati per qualsivoglia finalità, eccezion fatta solo per determinate finalità (ove il consenso privacy riguardi quelle determinate categorie di dati e sia prestato per finalità diverse da quelle eccezionalmente ammesse), quanto i consensi privacy prestati a fronte di specifici divieti di trattamento di determinate categorie di dati personali per certe finalità al di fuori di determinate circostanze fattuali e limiti temporali, che comportano, di converso, l'autorizzazione al trattamento solo entro certi limiti fattuali, ivi compresi certi limiti temporali.

## 5. Esempi.

### 5.1. Primo esempio: il consenso privacy esplicito illecito ex art. 9(2)(a) GDPR

L'art. 9(2)(a) GDPR prevede espressamente un esempio normativo di consenso privacy illecito, nel senso inteso nel presente scritto.

Come noto, il divieto del trattamento delle particolari categorie di dati di cui al paragrafo

1 dell'art. 9 GDPR può essere superato soltanto a certe condizioni, ossia su certe basi, tra cui quella del consenso «esplicito». Come pure noto, tuttavia, l'art. 9(2)(a) aggiunge che tale consenso privacy esplicito non può valere a superare il divieto di cui al paragrafo 1 del medesimo articolo *laddove ciò non sia consentito alla stregua del diritto dell'Unione o del diritto nazionale applicabile*[25]. Ciò sta a significare che in costanza di una norma imperativa esterna al Regolamento, di diritto unitario o nazionale, che vieta il trattamento di quei dati personali in modo inderogabile, il consenso privacy è invalido in quanto illecito, con la conseguenza che ogni relativo trattamento sarebbe illecito.

È una manifestazione normativa della illiceità del consenso privacy di cui vado parlando.

[25] Il paragrafo 1 e il paragrafo 2, lett. a) dell'art. 9 GDPR, rubricato «Trattamento di categorie particolari di dati personali» così recano: «1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. 2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, *salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1*; […]».



ISSN 2239-8570

### 5.2. Secondo esempio: il divieto dell'art. 26(3) DSA

L'art. 26(3) DSA prevede che i fornitori di piattaforme online non possono presentare pubblicità ai destinatari del servizio basate sulla profilazione (come definita nel GDPR) utilizzando le categorie speciali di dati personali di cui all'articolo 9(1) GDPR.

Tale norma prevede dunque uno specifico divieto di trattamento di una determinata categoria di dati personali per una determinata finalità rivolto a determinati destinatari, tale per cui debbono ritenersi invalidi in quanto illeciti i consensi privacy che siano prestati per questo trattamento vietato.

### 5.3. Terzo esempio: il divieto dell'art. 18(1)(c) del regolamento sul targeting della pubblicità politica

Similmente, l'art. 18(1)(c) del recente regolamento (UE) 2024/900 sulla trasparenza e il targeting della pubblicità politica[26] vieta le tecniche di targeting o di consegna del messaggio pubblicitario in ambito di pubblicità politica online che si avvalgano di tecniche di profilazione (come definita nel GDPR) utilizzando le categorie speciali di dati personali di cui all'articolo 9(1) GDPR.

Anche in questo caso dovremo dire che siamo in presenza di una norma che prevede uno specifico divieto di trattamento di una determinata categoria di dati personali per una determinata finalità, tale per cui devono ritenersi invalidi in quanto illeciti i consensi privacy che siano prestati per questo trattamento vietato.

### 5.4. Quarto esempio: i divieti dell'art. 7 della direttiva sui lavoratori delle piattaforme online

L'art. 7 della direttiva, recentemente adottata, relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali[27], *inter alia* vieta alle piattaforme di lavoro digitali (come ivi definite) di trattare mediante sistemi decisionali o di monitoraggio automatizzati (come ivi definiti): (a) dati personali relativi allo stato emotivo o psicologico della persona che svolge un lavoro mediante piattaforme digitali; (b) dati personali relativi a conversazioni private; (c) dati personali quando la persona che svolge un lavoro mediante piattaforme digitali non sta svolgendo un lavoro mediante le stesse o non si sta offrendo per svolgerlo; (d) dati personali per prevedere l'esercizio di diritti fondamentali, compresi il diritto di associa-

[26] Regolamento (UE) 2024/900 del 13 marzo 2024 relativo alla trasparenza e al targeting della pubblicità politica.

[27] Si fa riferimento al testo della direttiva adottato dal Parlamento europeo e dal Consiglio dell'Unione europea, ma non ancora pubblicato sulla GU dell'UE alla data in cui il presente saggio è stato inviato per la pubblicazione (https://www.europarl.europa.eu/news/it/press-room/20240419IPR20584/riders-il-parlamento-adotta-la-direttiva-sul-lavoro-delle-piattaforme).



ISSN 2239-8570

zione, il diritto di negoziazione e di azioni collettive o il diritto all'informazione e alla consultazione, quali definiti nella Carta dei diritti fondamentali della Unione europea; (e) dati personali per desumere l'origine razziale o etnica, lo status di migrante, le opinioni politiche, le convinzioni religiose o filosofiche, la disabilità, lo stato di salute, comprese le malattie croniche o la sieropositività, lo stato emotivo o psicologico, l'adesione a un sindacato, la vita sessuale o l'orientamento sessuale di una persona; (f) i dati biometrici, come definiti nel GDPR, di una persona che svolge un lavoro mediante piattaforme digitali per stabilirne l'identità confrontandoli con i dati biometrici di persone memorizzati in una banca dati.

Anche in questo caso siamo in presenza di una disciplina che prevede specifici divieti di trattamento di dati personali, e tali divieti sono variamente articolati non soltanto relativamente alle categorie di dati personali ma anche relativamente alle finalità e alle circostanze fattuali del trattamento (v. par. 4 *supra*). Anche in questo caso devono ritenersi invalidi in quanto illeciti i consensi privacy che siano prestati per i trattamenti vietati.

### 5.5. Quinto esempio: i divieti di uso di sistemi di IA dell'art. 5 AI Act

L'art. 5 dell'AI Act (di seguito anche "AIA")[28] vieta *inter alia* l'uso di una serie di sistemi di intelligenza artificiale ("IA").

Poiché l'uso dei sistemi di IA richiede ed include il trattamento di dati personali per finalità di addestramento, convalida, prova e input[29], deve ritenersi che il divieto d'uso dell'art. 5 AIA è idoneo a far ritenere senz'altro illegittima qualunque finalità di trattamento dei dati personali connessa all'uso dei sistemi di IA sottoposti al medesimo divieto, con la conseguenza che devono ritenersi invalidi in quanto illeciti i consensi privacy che siano prestati per queste specifiche finalità di trattamento.

### 5.6. Sesto esempio: lo sfruttamento delle vulnerabilità del Sig. Leon

Il successivo esempio è tratto dalle Linee guida EDPB 8/2020 sul *targeting* degli utenti di social media (versione 2.0 del 13 aprile 2021), dove si parla del signor Leon che è fatto bersaglio di pratiche di raccolta di dati personali in grado di individuare le persone impulsive e di basso reddito, e quindi di algoritmi che su questa base decidono che persone come lui - persone (ritenute) impulsive e di basso reddito - sono il bersaglio ideale di pubblicità di scommesse online[30].

[28] Regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

[29] Vedi le relative definizioni all'art. 3, numeri 29), 30), 32) e 33) AIA.

[30] EDPB, Linee guida 8/2020 sul targeting degli utenti dei social media. Versione 2.0, adottate il 13 aprile 2021, 27: «Esempio 8 Il signor Leon ha indicato nella propria pagina di social media di essere interessato allo sport. Ha scaricato un'applicazione sul proprio cellulare

ISSN 2239-8570

Nelle medesime Linee guida si trova la conclusione che il Sig. Leon, fornendo un consenso privacy esplicito ai sensi dell'art. 22 GDPR potrebbe validamente autorizzare un trattamento dei suoi dati personali di questo tipo, permettendo così agli algoritmi di bersagliarlo in questo modo[31].

Se facciamo emergere il profilo del sindacato di liceità del consenso privacy, che richiede doverosamente di stabilire se le finalità di trattamento sono legittime o sono illegittime, si deve ritenere corretta la soluzione opposta a quella delineata dall'EDPB, in quanto, nell'esempio del Sig. Leon, la finalità di trattamento dei dati personali consistente – come riconosciuto dallo stesso EDPB nelle Linee guida in commento – nello *sfruttamento delle vul-*

per seguire gli ultimi risultati degli incontri sportivi preferiti, ha impostato sul proprio browser la pagina www.risultatisportiviintemporeale.com come homepage sul suo portatile, usa spesso il desktop di cui dispone sul luogo di lavoro per cercare gli ultimi risultati sportivi su internet. Visita inoltre anche un certo numero di siti web di gioco d'azzardo online. Il fornitore di social media traccia l'attività online del signor Leon sui suoi molteplici dispositivi, ossia sul computer portatile, sul cellulare e sul deskto Sulla base di tale attività e di tutte le informazioni fornite dal signor Leon, il fornitore di social media deduce che sarà interessato alle scommesse online. *Inoltre la piattaforma di social media ha sviluppato criteri di targeting che consentono alle imprese di rivolgersi in maniera mirata a persone che probabilmente sono impulsive e hanno un reddito più basso*. La società di scommesse online "miglioriprestitiquotidiani" desidera rivolgersi agli utenti che sono interessati alle scommesse e che probabilmente scommettono somme considerevoli. Seleziona quindi i criteri offerti dal fornitore di social media per rivolgersi in maniera mirata al pubblico al quale dovrebbe essere mostrata la sua pubblicità» (https://www.edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_it_0.pdf).

[31] Le Linee guida 8/2020 in commento proseguono così argomentando a p 28-29: «Per quanto riguarda l'esempio 8, l'EDPB ricorda che nel caso di un processo decisionale automatizzato che produce effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona, come stabilito dall'articolo 22 del GDPR, i titolari del trattamento possono avvalersi delle seguenti eccezioni: • consenso esplicito dell'interessato; […]. Il Gruppo di lavoro ha già dichiarato che "*[i]n numerosi casi tipici, la decisione di proporre pubblicità mirata basata sulla profilazione non inciderà in modo analogo significativamente sulle persone [...]. Tuttavia è possibile che ciò possa accadere, a seconda delle particolari caratteristiche del caso, tra le quali: • l'invasività del processo di profilazione, compreso il tracciamento delle persone su siti web, dispositivi e servizi diversi*; • *le aspettative e le volontà delle persone interessate; • il modo in cui viene reso disponibile l'annuncio pubblicitario; oppure • lo sfruttamento della conoscenza di vulnerabilità degli interessati coinvolti*". Se la profilazione effettuata dal fornitore di social media può "[incidere] in modo analogo significativamente" su un interessato, si applica l'articolo 22. Il titolare del trattamento (o i contitolari del trattamento, a seconda del caso) dovrà (dovranno) effettuare una valutazione dell'eventualità che il *targeting* "[incida] in modo analogo significativamente" su un interessato, in ogni caso tenendo conto delle caratteristiche concrete del *targeting*. In tali circostanze, come descritto nell'esempio 8, la presentazione di pubblicità di scommesse online può rientrare nell'ambito di applicazione dell'articolo 22 GDPR (attività di *targeting* rivolta a persone finanziariamente vulnerabili interessate a scommesse online, che ha il potenziale di incidere significativamente e negativamente sulla loro situazione finanziaria). Di conseguenza, conformemente all'articolo 22, sarebbe necessario un consenso esplicito. Inoltre l'utilizzo di tecniche di tracciamento fa scattare l'applicabilità dell'articolo 5, paragrafo 3, della direttiva e-privacy, rendendo necessario il preventivo consenso da parte dell'interessato. Infine l'EDPB ricorda che il titolare del trattamento deve condurre una valutazione caso per caso rispetto alla liceità del trattamento, e che l'ottenimento del consenso non riduce gli altri obblighi relativi al rispetto delle prescrizioni in materia di correttezza, necessità, proporzionalità e qualità dei dati, di cui all'articolo 5 GDPR».



ISSN 2239-8570

*nerabilità* del Sig. Leon, è da ritenersi senz'altro illegittima perché in contrasto con il divieto generale delle pratiche commerciale scorrette di cui all'art. 5 della UCPD (la direttiva 2005/29/CE sulle pratiche commerciali scorrette) e con il divieto delle pratiche commerciali aggressive in particolare[32].



Pertanto l'eventuale consenso privacy, anche se esplicito ex art. 22 GDPR, del Sig. Leon deve ritenersi invalido in quanto illecito, perché prestato per una specifica finalità illegittima.

### 5.7. Settimo esempio: la piattaforma illegale di concorsi a premi

Volendo ora fare un esempio di contrasto delle specifiche finalità di trattamento con norme imperative di diritto nazionale (un secondo esempio è contenuto nel paragrafo successivo: v. par. 5.8 *infra*), possiamo fare quello di una piattaforma online che raccoglie dati personali sulla base del consenso per organizzare concorsi a premio *in violazione della normativa nazionale che regola i concorsi a premi*. Ben si danno nella realtà casi di piattaforme che non rispettano o che non rispettano integralmente la normativa di diritto pubblico che impone requisiti e limiti ai concorsi a premio[33].

[32] V. Comunicazione della Commissione "Orientamenti sull'interpretazione e sull'applicazione della direttiva 2005/29/CE del Parlamento europeo e del Consiglio relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno" (2021/C 526/01) pubblicata sulla Gazzetta Ufficiale dell'Unione Europea del 29.12.2021, che riporta - in una serie di casistiche di pratiche da ritenersi sleali e quindi proibite ai sensi della UCPD - esempi di sfruttamento di vulnerabilità decisionale dei consumatori esattamente di questo tipo (v. il primo riquadro di esempi al par. 4.2.7, ed in particolare il primo esempio: «Un professionista riesce a capire che un adolescente è in uno stato d'animo vulnerabile a causa di eventi accaduti nella sua vita personale. Tali informazioni sono successivamente utilizzate per raggiungere l'adolescente con messaggi pubblicitari basati sulle emozioni in un momento specifico»). Sembra anche significativo osservare come il profilo funzionale sulle specifiche finalità di trattamento sia stato ritenuto rilevante dallo stesso EDPB in un parere congiunto questa volta con l'EDPS (il Garante europeo della protezione dei dati) sulla proposta di AI Act del 2021. In quel parere di appena due mesi successivo alle Linee guida in commento si legge una netta critica della previsione della proposta di AI Act di "sdoganare", per così dire, generalmente i sistemi di intelligenza artificiale di rilevamento delle emozioni. In quel parere, al contrario si raccomanda un divieto generalizzato di sistemi di IA di questo tipo salvo che per casi d'uso ben specificati, ossia si raccomanda di ammetterli solo per specifiche finalità sanitarie o di ricerca (ad esempio per pazienti per i quali il riconoscimento delle emozioni è rilevante per fini di assistenza e cura). Si legge in particolare nel Parere congiunto EDPB-GEPD 5/2021 del 18 giugno 2021, sulla proposta di Artificial Intelligence Act, al punto 35 «[…] l'EDPB e il GEPD ritengono che l'utilizzo dell'IA per dedurre le emozioni di una persona fisica sia assolutamente inopportuno e dovrebbe essere vietato, ad eccezione di taluni casi d'uso ben specificati, ossia per finalità sanitarie o di ricerca (ad esempio pazienti per i quali il riconoscimento delle emozioni è rilevante), sempre applicando idonee tutele e, naturalmente, nel rispetto di tutte le altre condizioni e restrizioni relative alla protezione dei dati, compresa la limitazione delle finalità».

[33] V. il caso di cui al già menzionato provvedimento prescrittivo e sanzionatorio del Garante per la protezione dei dati personali nei confronti di Ediscom S.A. del 23 febbraio 2023 [doc- web 9870014].



ISSN 2239-8570

A mio avviso non c'è alcun dubbio che in un simile caso anche laddove gli utenti forniscano un consenso libero, specifico, informato e non ambiguo debba ritenersi che esso sia invalido in quanto rivolto a finalità di trattamento illegittime.



### 5.8. Ottavo esempio: i divieti di trattamento della legge sull'oblio oncologico

Tra gli ulteriori casi di consensi privacy illeciti, perché prestati per trattamenti espressamente vietati dal legislatore, si può far riferimento, nel diritto italiano, alla recente legge sull'oblio oncologico, la legge 193/2023[34].

Al centro della legge 193/2023 stanno le informazioni relative allo stato di salute della persona fisica concernenti patologie oncologiche da cui la stessa sia stata precedentemente affetta e il cui trattamento attivo si sia concluso, senza episodi di recidiva, da più di dieci anni o da più di cinque anni nel caso in cui la patologia sia insorta prima del compimento del ventunesimo anno di età.

L'art. 2 della legge 193/2023 vieta l'acquisizione e in ogni caso l'utilizzazione di tali informazioni relative ad una persona fisica contraente ai fini della determinazione delle condizioni contrattuali di qualunque tipo contratto, anche esclusivamente tra privati[35].

L'art. 3 della legge 193/2023 introduce una serie di modifiche alla legge 4 maggio 1983, n. 184, in materia di adozione, vietando l'acquisizione e l'utilizzazione delle medesime informazioni relative alle persone che intendono adottare.

L'art. 4 della legge 193/2023 vieta di richiedere le stesse informazioni relative a candidati ai fini dell'accesso a procedure concorsuali e selettive, pubbliche e private, anche quando nel loro ambito sia previsto l'accertamento di requisiti psico-fisici o concernenti lo stato di salute dei candidati.

Anche qui, non avrei dubbi nel ritenere invalido in quanto illecito ogni eventuale consenso privacy prestato dall'interessato a fronte delle condizioni che vietano il trattamento dei suoi dati personali consistenti nelle predette informazioni, ai sensi di questa disciplina.

### 5.9. Et cetera

Gli esempi si possono moltiplicare guardando sia ulteriori casi che non propongono difficoltà di interpretazione (consensi privacy relativi a tratta-

[34] Legge 7 dicembre 2023, n. 193 *Disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti delle persone che sono state affette da malattie oncologiche*.

[35] La precisazione che il divieto riguarda anche la contrattazione tra privati esclude ogni possibilità di ricostruire il divieto come basato sulla considerazione di posizioni di debolezza contrattuale tipicamente ravvisate in situazioni di contrattazioni tra imprese e consumatori, e dunque esclude la possibilità di ricostruire la *ratio* del divieto in termini di tutela della libertà del consenso privacy.



ISSN 2239-8570

menti espressamente vietati dalla legge) sia a quelli che invece richiedono uno sforzo interpretativo per stabilire se una determinata finalità di trattamento di dati personali debba ritenersi illegittima, in assenza di una norma di legge che espressamente la dichiari tale o che espressamente vieti il trattamento dei dati personali. Una conclusione nel senso del divieto di trattamento di dati personali potrà ricavarsi ermeneuticamente di volta in volta in presenza di norme che (pur non vietando direttamente determinati trattamenti di dati personali) vietano determinati comportamenti o processi automatizzati i quali comportano determinati trattamenti di dati personali.

I casi sono destinati a crescere con la legislazione orientata al governo dell'industria dei dati e all'apposizione di argini giuridici alle cosiddette decisioni automatizzate e alle applicazioni digitali di tecniche che nei più varî settori utilizzano i risultati delle neuroscienze[36].

Aggiungo qui soltanto in maniera sintetica - ma spero che si capisca il contesto discorsivo dell'accenno - che anche alcuni dei più importanti tra i recenti provvedimenti del Garante privacy italiano, quali quelli sulla chatbot Replika per i bambini[37] e su ChatGPT[38] confermano questa necessaria ten-

[36] Cfr. A.A. MOLLO, Neurorights. *Una prospettiva di analisi interdisciplinare tra diritto e neuroscienze*, in *Annuario 2022*, cit., 191 ss.; ID., *La vulnerabilità tecnologica.* Neurorights *ed esigenze di tutela: profili etici e giuridici*, in *European Journal Of Privacy Law & Technologies,* 2021, 199 ss.; con specifico riferimento al neuromarketing, cfr. AA.VV., *Annuario 2023-2024 Osservatorio Giuridico sull'innovazione digitale*¸ a cura di S. Orlando e G. Capaldo, in corso di pubblicazione, e v. anche lo studio del marzo 2023 intitolato *State of the art of neuromarketing and its ethical implications*, commissionato e pubblicato dalla Commissione europea (https://oeuropa.eu/en/publication-detail/-/publication/43754ac8-26aa-11ee-a2d3-01aa75ed71a1/language-en).

[37] 'Replika' è una applicazione di intelligenza artificiale di tipo conversazionale che genera un personaggio virtuale programmato per instaurare conversazioni, quasi del tutto realistiche, con gli utenti e per stringere con essi legami che replicano i rapporti di amicizia o anche le relazioni sentimentali tra gli esseri umani. Secondo la presentazione dei suoi sviluppatori, tale applicazione è "capace di migliorare l'umore ed il benessere emotivo dell'utente, aiutandolo a comprendere i suoi pensieri e i suoi sentimenti, a tenere traccia del suo umore, ad apprendere capacità di *coping* - ossia, di controllo dello stress - a calmare l'ansia e a lavorare verso obiettivi come il pensiero positivo, la gestione dello stress, la socializzazione e la ricerca dell'amore". Con provvedimento n. 39 del 2 febbraio 2023, l'Autorità garante per la protezione dei dati personali ha disposto, con effetto immediato, la limitazione provvisoria del trattamento dei dati personali degli utenti stabiliti nel territorio italiano, nei confronti della società statunitense Luka Inc., sviluppatrice e gestrice della chatbot 'Replika', in considerazione dei concreti rischi che l'impiego di tale app presenta nei confronti dei minori di età e dei soggetti più fragili dal punto di vista emotivo (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9852506). E v. anche il successivo provvedimento sospensivo condizionato n. 280 del 22 giugno 2023 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10013893).

[38] La prima misura cautelare adottata dal Garante per la protezione dei dati personali nei confronti di OpenAI per il servizio ChatGPT con provvedimento n. 112 del 30 marzo 2023 risulta motivata, *inter alia*, come segue: «l'assenza di filtri per i minori di età di 13 anni espone gli stessi a risposte assolutamente inidonee rispetto al grado di sviluppo e autoconsapevolezza degli stessi» (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832). E v. anche il successivo provvedimento sospensivo condizionato n. 114 dell'11 aprile 2023 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702) ed il comunicato stampa del 29 gennaio 2024 sulla notifica di



ISSN 2239-8570

sione verso un sindacato di legittimità sulle finalità del trattamento[39], che non è sempre agevole e che peraltro comporta, come accenneremo brevemente infra, delicate questioni di coordinamento tra diverse autorità (v. *infra* par. 7.2).



## 6. L'invalidità del consenso privacy per illiceità è idonea a tutelare sia l'interessato che soggetti terzi

Deve sottolinearsi che l'invalidità del consenso privacy per difetto del requisito di liceità è idonea a tutelare sia l'interessato (dei cui dati personali si tratti) che soggetti terzi, come nel caso dell'illiceità dei consensi privacy prestati per finalità di addestramento, convalida o prova dei sistemi di intelligenza artificiale sottoposti al divieto di uso ai sensi dell'art. 5 AI Act (v. *supra* par. 5.5).

Ed infatti, l'uso dei sistemi di intelligenza artificiale sottoposti al relativo divieto è considerato dal legislatore idoneo a ledere i diritti di una pluralità di persone e non solo quelli degli interessati, i cui dati personali siano processati dai sistemi di intelligenza artificiali vietati.

Gli interessati, in ipotesi, *possono non essere minacciati in alcun modo* dai sistemi di IA sottoposti al divieto di uso.

Per fare un esempio: se vengono raccolti con il loro consenso i dati personali di *persone non impulsive* per la finalità di addestrare, convalidare o provare un sistema di IA disegnato per manipolare il comportamento di *persone impulsive* sfruttando la loro vulnerabilità comportamentale derivante dall'impulsività, e che può così distorcere il loro comportamento e provocare loro un significativo danno ai sensi dell'art. 5(1)(a) AI Act, quei consensi privacy prestati dalle *persone non impulsive* dovranno senz'altro ritenersi invalidi in quanto illeciti anche se non è in gioco la lesione di loro diritti.

## 7. Tre aree di approfondimento.

contestazione di violazione del GDPR (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020). A proposito della protezione dei minori con riferimento alla legislazione sulla protezione dei dati personali cfr. *ex multis* i contributi di I.A. CAGGIANO, *Protecting minors as technologically vulnerable persons through data protection: An analysis on the effectiveness of law.*, 2022, in *European Journal of Privacy Law & Technologies* 27 ss.; F. RUGGERI, *Trattamento dei dati personali e tutela dei minori*, in *Annuario 2022*, cit, 325 ss. Più in generale sul tema della protezione "identitaria" dei minori nell'ambiente digitale R. SENIGAGLIA, *Rischi identitari per la persona minore di età nell'ambiente digitale*, in *European Journal of Privacy Law & Technologies*, 2023, 62 ss.; I. GARACI, *Autodeterminazione e tutela del minore di età nel contesto digitale*, in *Saggi di diritto dei consumi* a cura di A. Catricalà, M. Pignalosa, 2020, Giappichelli, Torino, 115 ss.; e anche, con specifico riferimento alle tematiche del marketing, ID., *Profili di tutela delle persone vulnerabili nell'ecosistema digitale. Il divieto di profilazione dei minori di età ai fini di marketing*, in *Annuario 2022*, cit., 89 ss.; ID., *Minori e pubblicità mirata*, in *Dir. Merc. e Tecnologia*, 2022, 1 ss.

[39] Cfr. anche la Relazione annuale 2023 del Presidente del Garante per la protezione dei dati personali Prof. Pasquale Stanzione *Regolare il futuro. La protezione dei dati per un'innovazione antropocentrica*, 8 ss.



ISSN 2239-8570

L'ipotesi costruttiva in parola apre tre prospettive di indagine a dir poco vaste.



### 7.1. La finestra con vista fuori del GDPR (il test di legittimità delle finalità di trattamento non è solo endo-regolamentare)

La prima corrisponde metaforicamente ad *aprire una finestra con vista fuori del GDPR*, perché, come argomentato, il test di liceità, comportando un giudizio sulla legittimità delle finalità del trattamento e una valutazione sul se il trattamento non sia altrimenti vietato (v. parr. 3, 4, 5 *supra*), non è solo endo-regolamentare bensì deve essere condotto alla stregua di tutte le altre norme imperative del diritto dell'Unione e del diritto nazionale applicabile.

Come già visto, la necessità di guardare fuori dal GDPR è imposta innanzitutto implicitamente dal combinato disposto dell'art. 5(1)(b)GDPR con l'art. 6(1)(a) GDPR (v. parr. 3 e 4 *supra*), ma anche espressamente nell'art. 9(2)(a) GDPR a proposito del consenso esplicito (v. par. 5.1 v), dove si prescrive che il consenso esplicito può superare il divieto del trattamento delle particolari categorie di dati ivi previste solo se questo non sia a sua volta vietato da altre norme del diritto dell'Unione o degli Stati membri. Dunque una finestra aperta in questo caso espressamente sulle altre norme del diritto dell'Unione o degli Stati membri. E lo stesso deve ritenersi senz'altro anche per l'altro consenso esplicito dell'art. 22(2)(a) GDPR. Ci torneremo brevemente più avanti (v. par. 7.3 *infra*). Qui è importante ribadire che è lo stesso GDPR - con il combinato disposto dei suoi artt. 5(1)(b) e 6(1)(a) e con il suo art. 9(1)(a) - ad aprire ora implicitamente ora espressamente una finestra sulle altre norme imperative del diritto unitario e nazionale applicabile per stabilire se le finalità del trattamento dei dati personali per le quali sia prestato il consenso privacy siano legittime e se il relativo trattamento non sia altrimenti vietato da norme inderogabili.

### 7.2. La questione della distribuzione di competenze tra autorità amministrative e giurisdizionali in relazione all'accertamento della legittimità/illegittimità delle finalità del trattamento

La seconda prospettiva di indagine, altrettanto ampia, riguarda *il tema di distribuzione di competenze su chi decide quali finalità di trattamento sono illegittime e quali trattamenti dei dati personali sono altrimenti vietati*. Ed infatti, se riconosciamo che il GDPR richiede di aprire una finestra sulle altre norme del diritto dell'Unione e nazionale, deve essere affrontato e risolto il tema del coordinamento tra le attività delle autorità di controllo designate per l'applicazione del GDPR nei paesi membri (le varie "DPA") e quelle delle varie autorità amministrative e giurisdizionali che hanno competenze di accertamento e sanzionatorie nei vari settori dell'ordinamento. Naturalmente c'è un livello nazionale di approfondimento e di svolgimento di que-



ISSN 2239-8570

sto tema, che riguarda la particolare distribuzione di competenze tra autorità nazionali, sulla base degli ordinamenti e delle norme di diritto pubblico degli Stati membri, ma c'è anche il livello del diritto dell'Unione, interpretando il quale soltanto possono essere individuate le linee generali di soluzione del problema, avuto riguardo al coordinamento tra le autorità previste dalle fonti di diritto unitario[40]. Può il Garante verificare da sé l'illegittimità delle finalità dei trattamenti dei dati personali o deve coordinarsi con altre autorità? Può o deve prendere per buone decisioni già esistenti ovvero deve chiedere decisioni di autorità giurisdizionali o di altre autorità che possono essere competenti per stabilire, come negli esempi che ho fatto prima, se un certo trattamento di dati personali è piegato a finalità illegittime o deve ritenersi altrimenti vietato sulla base di norme imperative che proibiscono determinate attività in settori presidiati da altre autorità? Si propone dunque un grande tema di coordinamento. Che si amplificherà, man mano che nuove autorità si aggiungeranno alle esistenti, come già si vede.

### 7.3. La ricerca della cassetta degli attrezzi più adeguata per affrontare le sfide ermeneutiche del consenso privacy nella data economy

Si propone, infine, un tema di svolgimento logico, che richiede innanzitutto di mettersi d'accordo su quale sia lo strumentario giuridico (la "cassetta degli attrezzi") più adeguato per trasferire sul piano dell'atto del consenso privacy il controllo di liceità, che è letteralmente riferito nel GDPR solo al trattamento.

La mia convinzione è che la teoria degli atti di autonomia privata fornisca lo strumentario più adeguato per compiere questo lavoro. E che, in questo senso, e per questo motivo, la teoria degli atti autonomia privata – se rettamente intesa - piuttosto che costituire una minaccia di mercificazione dei dati personali, sia, al contrario, capace di fornire una risposta di protezione.

Sembra pertinente osservare in proposito che, per attribuire validità all'atto di autonomia privata, si guarda sempre alla libertà e alla consapevolezza del suo autore, ma *anche* al profilo funzionale dell'atto, consentendo un sindacato di liceità orientato alla protezione del più ampio complesso di valori riconosciuti dall'ordinamento nella sua funzione di postulazione e affermazione deontica degli interessi dell'intera collettività[41]: ampliando così

[40] Cfr. la sentenza CGUE del 4.7.2023 nel caso C-252/21 e le pertinenti osservazioni di P. STANZIONE, *La libertà e il suo valore*, cit., 155.

[41] Cfr. P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., 415, dove il principio di liceità del *trattamento* è interpretato come base normativa per «selezionare i trattamenti ammessi dall'ordinamento»; e v. anche ivi, 412-413 dove osserva che il corrispondente giudizio di liceità ha per caratteristica di «contemplare una valutazione di interessi che opera su un piano (anche superindividuale e che, là dove guardi alla posizione della singola parte del rapporto (l'interessato in primo luogo), sia in grado di prescindere dalle preferenze di quest'ultimo, in ipotesi in cui queste contrastino con l'interesse della collettività». Si tratta di osservazioni pertinenti ove si osservi che la legittimità delle finalità del trattamento - rilevanti per il consenso privacy nel senso detto, per il combinato disposto delle disposizioni di cui agli artt. 5(1)(b) e 6(1)(a) GDPR – va asseverata, naturalmente, sul-



ISSN 2239-8570

la considerazione rilevante per il giudizio di rilevanza e di tutela giuridica ben *oltre* l'ambito della protezione dei valori della libertà e della consapevolezza dell'autore dell'atto.

Deve in proposito riconoscersi che le discipline del consenso negoziale tradizionalmente contemplano requisiti di libertà e consapevolezza degli autori dell'atto di autonomia, proteggendo sempre, senza incertezze, i medesimi requisiti a cospetto di situazioni nelle quali si rinviene la necessità della loro protezione (ed articolando variamente le discipline con norme di generalità variabile intese a contrastare in ciascun caso comportamenti contrari a buona fede, anche in relazione a situazioni nelle quali il legislatore vede una minaccia di quei requisiti, come nei casi di approfittamento di situazioni di asimmetria informativa e altre situazioni di vulnerabilità decisionale)[42]; ma, anche che, *in aggiunta a ciò*, la teoria degli atti di autonomia privata prevede e impone sempre un controllo funzionale: sulla funzione dell'atto. Ed è un controllo, per così dire, ordinamentale, a protezione degli interessi della collettività.

Quindi libertà e consapevolezza dell'autore dell'atto, innanzitutto, ma al contempo anche liceità.

Esiste già d'altronde, come visto, una disposizione del GDPR che impone *espressamente* un controllo di liceità del consenso privacy. Laddove, come detto, un simile controllo deve ritenersi *implicitamente* richiesto *sempre* - alla stregua dell'art. 6(1)(a) GDPR in combinato disposto con l'art. 5(1)(b) GDPR - esso è invece *espressamente* prescritto a proposito del consenso (privacy) «esplicito» ex art. 9(2)(a) GDPR.

Ed infatti come già osservato (v. parr. 5.1 e 7.1 *supra*) l'art. 9 del Regolamento, prevedendo al secondo paragrafo che il «consenso esplicito» possa permettere di superare il divieto del trattamento delle particolari categorie di dati elencate nel primo paragrafo, aggiunge però che un simile consenso esplicito può far superare quel divieto a meno che tale superamento ad opera di un consenso esplicito dell'interessato *non sia a sua volta vietato da altre norme di diritto dell'Unione o degli Stati Membri*.

Come anche detto, qui è inequivocabilmente disegnata una finestra che si affaccia fuori dal Regolamento (par. 7.1 *supra*).

Cosa che – aggiungo ora – a mio avviso deve ritenersi assolutamente sottintesa (tale e quale) anche nell'art. 22(2) GDPR.

Ed infatti - ferme restando le finalità proprie dell'art. 22 GDPR nel disegno del Regolamento e fermi restando i limiti intrinseci delle c.d. decisioni automatizzate e la loro pericolosità derivante dalle loro connaturate irrazionalità ed idoneità a realizzare discriminazioni: tratti ben messi in luce di re-

---

la base della liceità del trattamento, nel senso che non può considerarsi una finalità legittima di trattamento quella di un trattamento vietato da altre norme di legge (v. *retro*, parr. 3 e 4).

[42] Non è vero che esiste un consenso negoziale monolitico (quanto ai requisiti legali) da contrapporre a quello privacy, nemmeno restringendo la considerazione dell'autonomia privata all'ambito patrimoniale. Non è questa la sede per svolgere compiutamente questo tema. Ci si limita a richiamare in proposito le riflessioni esposte da ultimo proprio in relazione al dibattito del consenso privacy da G. FINOCCHIARO, *Consenso al trattamento e libertà*, cit., spec. 8 ss.; V. RICCIUTO, *Consenso al trattamento e contratto,* cit., spec. 20 ss.



ISSN 2239-8570

cente dalla dottrina più avvertita[43] - a mio avviso, sul piano della tecnica del rapporto tra il primo e il secondo paragrafo dell'art. 22 del Regolamento, va riconosciuto in ogni caso che la possibilità che il consenso esplicito (del secondo paragrafo dell'art. 22 GDPR) possa far superare il divieto (del primo paragrafo dell'art. 22 GDPR) deve essere intesa e qualificata esattamente come nell'art. 9 GDPR, ossia con esclusione dei casi in cui altre norme di diritto dell'Unione o degli Stati membri non consentono al consenso esplicito di superare il divieto di assoggettarsi a decisioni che producono effetti giuridici che lo riguardano o incidono sulla sua persona basate esclusivamente sul trattamento automatizzato dei dati personali[44].

Riconoscere un limite ordinamentale al consenso privacy è tanto più urgente nello scenario attuale che ha segnato in pochi anni il trapasso dalla società dell'informazione, caratterizzata dalla riproduzione e comunicazione automatizzate di dati digitali, alla *data driven economy* o *data economy*, caratterizzata dalla *produzione automatizzata di dati digitali* (in aggiunta alla riproduzione e alla comunicazione) attraverso il trattamento di altri dati, compresi, naturalmente, dati personali. Ed effettivamente, dati che rispondono alla qualificazione giuridica di dati personali vengono continuamente non soltanto forniti dall'interessato e riprodotti con sistemi automatizzati ma anche *prodotti* da sistemi automatizzati, compresi, oggi, in parte sempre maggiore, sistemi di intelligenza artificiale[45].

Postulare, come è ovvio, che possano e debbano esserci dei limiti a questa industria dei dati, non può prescindere dall'acquisizione di strumenti della tecnica giuridica idonei a tradurre quell'idea generica di limiti in divieti giuridici e la violazione di quei divieti in precise conseguenze sul piano del trattamento degli atti di autonomia privata. In altre parole, la generica consapevolezza dell'esistenza di limiti giuridici all'industria dei dati, deve necessariamente accoppiarsi alla consapevolezza della necessità di uno strumentario giuridico da esercitarsi sul piano dell'autonomia privata.

Individuato come piano di qualificazione e costruzione del consenso privacy l'atto di autonomia privata, si tratterà allora di affrontare una serie di questioni tecniche con la corrispondente cassetta degli attrezzi.

Si potrà così riconoscere che, a seconda del contesto nel quale si inserisce e viene prestato, l'atto di consenso privacy (sempre e in ogni caso inteso come atto di autonomia privata) può essere come può non essere qualificato come consenso contrattuale[46], ferma restando, anche nel caso in cui si tratti

[43] Cfr. per tutti D. IMBRUGLIA, *Le presunzioni delle macchine*, cit., 921 ss., spec. 930 ss. In termini più generali, A. SIMONCINI, Do ut data: *quali limiti costituzionali alla cessione di dati personali?*, in *Commerciabilità dei dati personali*, cit., 67; ID., *Il linguaggio dell'Intelligenza Artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, n. 2, 2023. V. anche G. CARAPEZZA FIGLIA, *Decisioni algoritmiche tra diritto alla spiegazione e divieto di discriminare*, in *Pers. Merc.*, 2023, 638 ss.; A.G. GRASSO, *GDPR Feasibility and Algorithmic Non-Statutory Discrimination*, Napoli, ESI, 2023.

[44] Nello stesso senso, D. IMBRUGLIA, *Le presunzioni delle macchine*, cit., 944-945.

[45] Cfr. S. ORLANDO, Data vs Capta*. Intorno alla definizione di dati,* in *Nuovo dir. civ.*, 2022/4, 14 ss., spec. 29 ss.; GUARDA, *Il regime giuridico dei dati della ricerca scientifica*, Trento, 2021, 11 ss., 25 ss.

[46] È la posizione affermata con chiarezza e con nettezza da V. RICCIUTO, *Consenso e contratto*, cit. *passim*. Nello stesso senso, anche S. ORLANDO, *Il coordinamento tra la Direttiva 2019/770 e il GDPR. L'interessato-consumatore*, cit. *passim*.



ISSN 2239-8570

di un consenso contrattuale, l'applicazione dell'intero statuto del GDPR, che interviene *a conformare e limitare in modo imperativo l'autonomia privata in questo settore*[47].

Si potrà sviluppare una teoria sulla granularità causale relativamente al requisito di specificità delle finalità di trattamento dei dati personali posto dall'art. 6(1)(a) GDPR, valorizzando in proposito le norme speciali confermative di questo requisito, come quelle del DSA che prevedono che i destinatari dei servizi di piattaforme online possano modificare i parametri della pubblicità ad essi rivolta e le opzioni che influenzano i parametri dei sistemi di raccomandazione che determinano l'ordine delle informazioni ad essi presentate[48].

Si potrà elaborare, in coerenza con la teoria sulla granularità causale delle specifiche finalità di trattamento per le quali il consenso privacy è prestato, una teoria sull'invalidità parziale del consenso privacy relativamente a quei casi in cui alcune delle specifiche finalità di trattamento dei dati personali per cui il consenso privacy è prestato siano illegittime mentre altre siano legittime.

Si potrà approfondire ulteriormente il requisito della specificità della finalità posto dall'art. 6(1)(a) GDPR interrogandosi sull'idoneità di assolvere a quel requisito da parte di consensi privacy prestati in adesione a richieste che, come quasi sempre avviene, formulano le finalità in modo generico (es. finalità di marketing, di pubblicità, etc.), per stabilire quale debba essere la conseguenza più coerente di un difetto del requisito della specificità[49] – anche avuto riguardo all'interesse dell'interessato – sul piano del trattamento del consenso privacy (anche qui, come può intuirsi, sul piano del trattamento del consenso privacy come atto di autonomia si può giocare sul piano del consenso – quale volontà informata e consapevole - o su quello della causa e dell'oggetto), eventualmente affacciando soluzioni che, similmente a quanto può proporsi di fronte al consenso prestato per specifiche finalità legittime e per specifiche finalità illegittime, concludano, laddove se ne ravvisi un interesse dell'interessato, per una validità/invalidità parziale, ossia per

[47] Parla espressamente di "*autonomia conformata* soggetta ai principi e precetti regolatori inderogabili del GDPR" E. TOSI, *Consenso autorizzatorio e consenso contrattuale quali autonome basi giuridiche per la patrimonializzazione dei dati personali nei mercati digitali alla luce del* GDPR, in *Commerciabilità dei dati personali,* cit., 229. E v. anche C. SOLINAS, *Autonomia privata e regolazione pubblica nel trattamento dei dati personali*, cit.; nonché, in una visione più generale: ID., *Il contratto "amministrato". La conformazione dell'operazione economica agli interessi generali*, Napoli, Esi, 2018; G. BERTI DE MARINIS, *Contratti dei mercati regolamentati: norme imperative e conformazione*, Napoli, Esi, 2019. V. anche S. SICA, *La monetizzazione dei dati tra autonomia privata e tutele civili*, in *Commerciabilità dei dati personali,* cit., 263.

[48] Artt. 26 e 27 DSA.

[49] Cass. 17278/2018, punto 2.6 "[…] Inoltre, ritiene il Collegio, perché il consenso possa essere detto specifico, che esso, per la contraddizione che non lo consente, non possa essere genericamente riferito a non meglio identificati messaggi pubblicitari, sicché colui il quale abbia chiesto di fruire di un servizio di informazioni giuridico-fiscali, si debba vedere poi raggiunto da pubblicità di servizi o prodotti non attinenti alle ricerche effettuate. È allora specifico, per questo aspetto, il consenso se riferito 'ad un trattamento chiaramente individuato', il che comporta la necessità, almeno, dell'indicazione dei settori merceologici o dei servizi cui i messaggi pubblicitari saranno riferiti".





ISSN 2239-8570

la validità del consenso privacy per la generalità delle finalità legittime comprese nella formula generica e per una corrispondente invalidità parziale limitatamente alle finalità *illegittime* che pure possono essere ricomprese nella medesima formula generica (l'esempio della formula generica della finalità di marketing o pubblicità è in proposito calzante, a fronte di specifici divieti in materia: v. i numerosi esempi al par. 5 *supra*).

Si potranno combinare insieme, in una visione funzionale, le categorie tradizionali (della tradizione dogmatica dell'atto di autonomia privata) dell'illiceità dell'oggetto e dell'illiceità della causa, in considerazione della varia articolazione dei divieti legali del contemporaneo diritto dei dati (v. parr. 4 e 5 *supra*), ed in particolare per corrispondere alla vasta tipologia dei divieti di trattamento rivolti a determinate categorie di dati personali. E così via.

Né sfuggirà che un'analisi simile può essere sviluppata *anche in relazione alla base del legittimo interesse* (art. 6(1)(f) GDPR)[50], non immune, come risaputo, dalla genericità (mi riferisco alla genericità del richiamo che ne fanno i titolari che si avvalgono di tale base, sfruttando l'ampiezza della formula legislativa), nel senso che mi sembra arrivato il momento di promuovere un sindacato di liceità *analitico* tanto sulle finalità del consenso che sul legittimo interesse, oltretutto in considerazione del fatto che oggi tanto è possibile anche dal punto di vista tecnologico, attraverso l'analisi puntuale degli algoritmi impiegati dai sistemi di intelligenza artificiale e dai sistemi software in generale[51].

## 8. Critica esemplare al Considerando 40 della direttiva sui lavoratori delle piattaforme online a dimostrazione della necessità di dismettere la concezione che si incentra esclusivamente sui requisiti di libertà e consapevolezza del consenso privacy

Prima di tracciare le conclusioni, mi sembra necessario aggiungere che la concezione c.d. autorizzatoria del consenso privacy, la quale si incentra esclusivamente sulla libertà e sulla consapevolezza dell'interessato, è ancora largamente dominante, ed al contempo indicare il limite storico di questa concezione, diventata ormai un abito mentale che ostacola il riconoscimento delle vere *rationes* di molti divieti che caratterizzano il diritto contemporaneo dei dati.

[50] Art. 6(1)(f) GDPR: «il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore».

[51] Cfr. D. MULA, *Elaborazione e sfruttamento dei dati mediante algoritmi*, in *La circolazione dei dati*, cit., spec. 148: "Al fine di determinare se un 'trattamento svolto tramite impiego di algoritmo' è conforme alla disciplina in materia di trattamento dei dati personali, deve, quindi, ritenersi legittima l'istanza di verifica, in concreto, delle attività svolte sia in relazione alla base giuridica dichiarata che rispetto all'eventuale ambito di consenso prestato dall'interessato […]".



ISSN 2239-8570

Il Considerando 40 della direttiva sulla tutela dei lavoratori delle piattaforme online[52] dimostra sia il perdurante dominio di questa concezione che la sua capacità ostacolante, nel senso detto. In esso si trova infatti scritto che i molti divieti al trattamento dei dati personali dei lavoratori delle piattaforme online, contenuti nell'art. 7 della medesima direttiva (v. par. 5.4 *supra*), sarebbero giustificati dalla situazione di assenza di una effettiva libertà di prestare il consenso privacy in cui si trovano tipicamente le persone che svolgono un lavoro mediante piattaforme digitali.

Il sottotesto di questa concezione è che, se fossero garantite effettive condizioni di libertà e consapevolezza alle persone che svolgono un lavoro mediante piattaforme digitali, o anche solo ad una categoria di tali persone, esse dovrebbero essere lasciate libere di consentire che sistemi decisionali o di monitoraggio automatizzati trattino loro dati personali relativi a loro stati emotivi o psicologici o relativi a loro conversazioni private, ivi inclusi dati riferibili al tempo in cui non lavorano, o per prevedere l'esercizio di loro diritti fondamentali (compresi il diritto di associazione, il diritto di negoziazione e il diritto di esercitare azioni collettive o il diritto all'informazione e alla consultazione), o anche per desumere la loro origine razziale o etnica, o il loro status di migrante, le loro opinioni politiche, le loro convinzioni religiose o filosofiche, loro eventuali disabilità, il loro stato di salute (comprese le malattie croniche o la sieropositività), il loro stato emotivo o psicologico, la loro adesione a sindacati, la loro vita sessuale o il loro orientamento sessuale.

La concezione autorizzatoria è dunque, evidentemente, ostacolante fino al punto da impedire perfino al legislatore europeo in sede di dichiarazione autentica della *ratio* dell'art. 7 della direttiva in commento, di sillabare la vera ragione di tutti questi divieti, e cioè che al diritto unitario ripugna un controllo automatizzato sui lavoratori di questo tipo ed una gestione automatizzata dei rapporti di lavoro di questo tipo, indipendentemente da qualunque consenso e anzi anche contro ogni eventuale consenso, libero e consapevole che sia.

Il consenso privacy non può essere il sinonimo di libertà di farsi perseguitare consapevolmente. Esistono dei limiti anche al consenso privacy libero e consapevole, che compete al legislatore fissare. La concezione del consenso privacy come atto di autonomia privata (o concezione negoziale) am-

[52] Considerando 40 della direttiva relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali: «Gli articoli 5, 6 e 9 del regolamento (UE) 2016/679 stabiliscono che i dati personali devono essere trattati in modo lecito, corretto e trasparente. Ciò comporta alcune restrizioni al modo in cui le piattaforme di lavoro digitali possono trattare i dati personali mediante sistemi decisionali e di monitoraggio automatizzati. Tuttavia, nel caso specifico del lavoro mediante piattaforme digitali, non si può presumere che il consenso delle persone che svolgono un lavoro mediante piattaforme digitali al trattamento dei loro dati personali venga dato *liberamente*. Spesso le persone che svolgono un lavoro di questo tipo *non hanno una reale libertà di scelta* o non possono rifiutare o revocare il consenso senza pregiudicare il loro rapporto contrattuale, visto lo squilibrio di potere tra la persona che svolge un lavoro mediante piattaforme digitali e la piattaforma di lavoro digitale. Pertanto, le piattaforme di lavoro digitali non dovrebbero trattare i dati personali delle persone che svolgono un lavoro mediante piattaforme digitali sulla base del fatto che una persona che svolge tale lavoro ha prestato il proprio consenso al trattamento dei suoi dati personali».



ISSN 2239-8570

mette questi limiti, anzi li postula come *necessari*, e consentirebbe (ovvero consentirà, quando cesserà, sperabilmente presto, il dominio della concezione che vede solo i requisiti di libertà e consapevolezza) anche allo stesso legislatore europeo di dichiararne le vere *rationes*.



## 9. Critica esemplare alla formula definitoria del diritto all'oblio oncologico nella legge 193/2023 a dimostrazione della necessità di evidenziare la figura logica del divieto che caratterizza il contemporaneo diritto dei dati

L'art. 1, co. 2 della legge 193/2023 contiene la seguente definizione di «diritto all'oblio oncologico»: «il diritto delle persone guarite da una patologia oncologica di non fornire informazioni né subire indagini in merito alla propria pregressa condizione patologica, nei casi di cui alla presente legge».

Tale formula definitoria non riflette le situazioni giuridiche soggettive che caratterizzano la disciplina introdotta dalla medesima legge, caratterizzata interamente, a ben vedere, dalla figura logica del divieto. La legge contiene una serie di divieti giustificati dalla previsione di minacce ad un diritto di rango costituzionale, il diritto a non essere discriminati, specificato, in casi circostanziati, come diritto delle persone fisiche a non essere discriminati a cagione della particolare condizione di una pregressa patologia oncologica. La legge 193/2023 contiene infatti una serie di divieti di comportamenti tipicamente ritenuti idonei a discriminare le persone fisiche a cagione di una loro pregressa patologia ontologica, e dunque a ledere questo diritto di rango costituzionale relativamente alla specifica condizione di salute considerata. Questi divieti sono formulabili come altrettanti divieti di trattamenti di determinate categorie di dati personali per determinate finalità.

La formula "diritto a non dare informazioni" così come quella di "diritto di non essere sottoposti ad indagini" non sono soltanto inidonee a riflettere le situazioni soggettive del divieto e del diritto costituzionale, che innervano invece la disciplina nel senso sopra esposto (e v. anche par. 5.8 *supra*). Esse sono anche fuorvianti, perché nascondono il carattere inderogabile della medesima disciplina.

In particolare, la formula "diritto a non dare informazioni" sembrerebbe suggerire che l'interessato può comunque darle, cosicché, in quel caso, chi le riceve potrebbe tenerne conto ai fini e nei campi di applicazioni considerati dalla legge. Ciò va escluso radicalmente. Di nuovo: si tratta di divieti inderogabili di trattamento di certi dati personali per determinate finalità. E, di nuovo: l'eventuale consenso privacy a trattare quei dati per quelle specifiche finalità, anche laddove libero e consapevole, sarebbe illecito.

Allo stesso modo, l'espressione "diritto di non essere sottoposti ad indagini" deve tradursi come: divieto di compiere indagini.

L'esegesi delle disposizioni contenute negli articoli da 2 a 4 della legge 193/2023, conferma che essa contiene solo divieti inderogabili, nel senso esposto, con tutte le conseguenze che devono ricavarsene sul punto del consenso privacy (v. *retro* par. 5.8).



ISSN 2239-8570

Più generalmente, e come fatto già nel paragrafo precedente a proposito del legislatore europeo, la critica a questa formula definitoria mi serve, prima delle conclusioni, per mettere in luce la perdurante difficoltà manifestata dallo stesso legislatore italiano di chiamare col suo nome la figura logica del divieto, che pure caratterizza nettamente il contemporaneo diritto dei dati e conforma l'autonomia privata in questo settore del diritto.



## 10. Conclusioni sul consenso privacy come atto di autonomia privata e sulla prospettiva di una nuova stagione di studi sull'atto di autonomia privata di diritto unitario sollecitata dallo studio dell'illiceità del consenso privacy.

Le osservazioni che ho provato ad esporre in questa sede possono compendiarsi in due riflessioni conclusive.

La prima è che l'autonomia privata non è da intendersi nel campo del trattamento dei dati personali come sinonimo di mercificazione dei dati personali[53], ma, tutt'al contrario, come un potenziamento della tutela della persona.

Lo studio del consenso privacy come atto di autonomia privata offre e richiede una tecnica (una "cassetta degli attrezzi") idonea ad individuare e a tutelare non soltanto gli insopprimibili diritti fondamentali dell'interessato, ma i diritti fondamentali di tutti i consociati.

Non solo, dunque, l'insopprimibile dignità di ciascuno e di tutti gli interessati, ma - accanto ed in aggiunta ad essa - il profilo di dignità - ancora da affermare – di una collettività di persone che distinguiamo oggi dalle comunità degli uomini del passato per il fatto di vivere in un mondo caratterizzato dall'ubiquità del software: in cui praticamente tutti i tipi di rapporti tra gli uomini sono potenzialmente mediati da applicazioni di tecnologie digitali, che continuamente ed in modo automatizzato riproducono e producono dati.

Le norme imperative sulla protezione e la circolazione dei dati personali hanno senz'altro in questo senso un ruolo di conformazione e di limitazione dell'autonomia dei privati.

Inoltre, nella prospettiva del consenso privacy quale atto di autonomia regolato e dunque necessariamente limitato, dovrà riconoscersi che i limiti al consenso privacy possono apprezzarsi soltanto attraverso la doverosa considerazione ed applicazione di tutte le norme imperative del diritto unitario e nazionale applicabile, che pongono precisi limiti all'industria dei dati. È la "finestra con vista fuori dal GDPR", cui ho fatto cenno *supra* (par. 7.1).

Come seconda riflessione conclusiva, sembra corretto dire che le categorie del divieto e della illiceità, con le quali il giurista europeo è tenuto a ci-

[53] Assolutamente condivisibili sono le analisi sui rischi di mercificazione dei dati personali nell'attuale assetto dei mercati digitali, che si leggono in P. STANZIONE, *La libertà e il suo valore*, cit., 149 ss., spec. 152; G. CERRINA FERONI, *Siamo stati derubati? Considerazioni (non conclusive) sul valore economico dei dati personali*, in *Commerciabilità dei dati personali*, cit. 413 ss., spec. 420 ss.; A. GHIGLIA, *Commerciabilità dei dati personali: condizioni e limiti alla monetizzazione della nostra identità digitale nel contesto italiano ed europeo*, ivi, 23 ss., spec. 29.

ISSN 2239-8570

mentarsi applicando il GDPR e le altre fonti da esso chiamate in causa per stabilire la legittimità delle finalità e dell'oggetto del trattamento, offrono ai giuristi europei la possibilità di un'elaborazione nuova e storicamente adeguata sull'autonomia privata nel diritto dell'Unione: una riflessione unitaria (nel senso del diritto dell'Unione europea) sulle categorie dell'autonomia privata.

Questa prospettiva consente infatti di guardare al consenso privacy come ad un banco di prova per costruire intorno ad esso una *teoria dell'atto di autonomia privata di diritto europeo*.

A chi si dicesse sorpreso che la proposta di un'elaborazione di una teoria generale dell'atto di autonomia privata di diritto europeo possa originare dall'interpretazione del GDPR, risponderei che la sorpresa è fuor di luogo, per almeno tre ordini di motivi.

Innanzitutto perché l'industria dei dati costituisce oggi il settore maggiormente in crescita nell'economia mondiale[54], e dunque non deve affatto sorprendere che a dare impulso ad una nuova stagione di studi del diritto europeo sull'autonomia privata possa essere l'analisi giuridica dei conflitti creati dalla *data economy*, a partire da quelli inerenti alla circolazione e alla protezione dei dati personali.

In secondo luogo, perché sembra corretto osservare che non siamo di fronte ad una vera opzione, in quanto le norme del GDPR *impongono* questa scelta. Ed infatti, come osservato, l'art. 5(1)(b) del Regolamento, contemplando ed *imponendo* un test di legittimità sulle specifiche finalità del trattamento dei dati personali, deve necessariamente accoppiarsi al profilo funzionale dell'atto di consenso privacy: perché, ai sensi dell'art. 6(1)(a) GDPR, l'interessato presta il consenso al trattamento «*per* una o più specifiche finalità»: che *devono*, dunque, essere «legittime», né può negarsi che assumano in proposito rilevanza tutte le norme dell'ordinamento, di diritto unitario e nazionale, che, in modo via via crescente, prendono atto della esigenza di regolare l'utilizzazione e la produzione dei dati digitali, e che interpretano questa esigenza attraverso la posizione di specifici divieti di trattamento di determinate categorie di dati personali nei più vari settori.

Infine, e non meno significativamente, perché mai come oggi, con poche multinazionali - i "gate-keeper"[55] - che dispongono di risorse finanziare e tecnologiche superiori a quelle della maggior parte degli Stati[56], è improro-

[54] Cfr. G. SMORTO, *Il ruolo della comparazione giuridica nella contesa per la sovranità digitale*, in *Esperienze giuridiche in dialogo*, cit. 75 ss.

[55] V. artt. 2 e 3 del *Digital Markets Act* (regolamento (UE) 2022/1925 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali))

[56] Nel comunicato stampa pubblicato sul sito web del Dipartimento di Giustizia degli Stati Uniti d'America (lo U.S. Department of Justice, Antitrust Division) a proposito di un'azione civile promossa il 21.3.2024 dal medesimo Dipartimento di Giustizia unitamente a 16 procuratori statali e distrettuali contro Apple Inc. per avere quest'ultima società pretesamente monopolizzato, o tentato di monopolizzare, i mercati connessi all'utilizzo e sviluppo degli smartphone, viene specificato che nell'anno fiscale 2023, Apple ha generato ricavi netti per 383 miliardi di dollari e un utile netto di 97 miliardi di dollari, sottolineandosi che l'utile netto di Apple supera il prodotto interno lordo di più di 100 paesi (https://www.justice.gov/opa/pr/justice-department-sues-apple-monopolizing-smartphone-markets).



ISSN 2239-8570

gabile l'avvio di una nuova stagione di studî sulle funzioni degli atti di autonomia, sulla loro legittimità e sull'invalidità intesa esattamente come reazione dell'ordinamento alla violazione di specifici divieti. Uno studio storicamente avvertito sull'autonomia privata deve principiare oggi dalle categorie del divieto e della illiceità.

Sembra in proposito necessario mutarsi, perfino nel linguaggio, la concezione corrente (e che non è mai stata tecnicamente corretta) dell'autonomia privata affidata unicamente alla parola libertà (libertà negoziale, contrattuale, *freedom of contract*), disvelando, insieme alla sua dimensione di libertà, quella del dovere – due facce della stessa medaglia, l'autonomia privata essendo un potere regolato, ossia limitato dal diritto - in particolare sotto la forma del divieto: il dovere di non fare[57].

Nell'erigendo diritto europeo dei dati, il divieto è manifestato oggi in numerose norme imperative che pongono limiti precisi all'industria dei dati.

Le linee di disvelamento della faccia del divieto nella disciplina dell'autonomia privata, insieme a quella della libertà, sono ormai progressivamente sempre più evidenti nell'elaborazione della dottrina europea sugli atti di autonomia privata, anche se fin qui non si è consolidata una speculazione di questo tipo sui contratti e sugli atti di autonomia caratteristici del diritto dei dati, e sul consenso privacy in particolare[58].

---

[57] Cfr. S. ORLANDO, *Fattispecie, comportamenti, rimedi. Per una teoria del fatto dovuto*, in *Riv. trim. dir. proc. civ.*, 2011, 1033 ss. spec. 1052 ss.

[58] Per delle osservazioni critiche sul ruolo che il sindacato sul consenso ha assunto nel diritto privato contemporaneo, v. M. FABRE-MAGNAN, *L'institution de la liberté*, Paris, 2023 (2 ed.). Nell'ambito degli studi sull'autonomia privata, la dottrina europea ha indagato il tema dei limiti alla libertà dei privati con primario riferimento alla c.d. *freedom of contract*. Sul punto, oltre al fondamentale S. ATIYAH, *The Rise and Fall of Freedom of Contract*, Oxford, 1985, si v., almeno, M.R. MARELLA, *The Old and the New Limits to Freedom of Contract,* in *European Review of Contract Law*, 2006, 257; J. BASEDOW, *Freedom of Contract in the European Union*, in *European Review of Private Law*, 2008, 901; N. REICH, *General Principles of EU Civil Law,* Cambridge, 2013, 17; O.O. CHEREDNYCHENKO, *Freedom of Contract in the Post-Crisis Era: Quo Vadis?,* in *European Review of Contract Law*, 2014, 390; ID., *Fundamental Freedoms, Fundamental Rights, and the Many Faces of Freedom of Contract in the EU*, in *The reach of free movement*, a cura di M. Andenas, T. Bekkedal, L. Pantaleo, Asser Press, The Hague, 2017, 273 ss.; G. VETTORI, *Diritto europeo e tutele contrattuali*, in *Pers. Merc.*, 2014, 89 ss.; S.J. WHITTAKER, *Introduction*, in *Chitty on Contracts, Volume I, General Principles*, 35 ed., Londra (Sweet & Maxwell), 2023, ove un'interessante rassegna dei limiti che tale principio incontra nel diritto inglese, tra cui i limiti discendenti dal diritto antidiscriminatorio. Per il riconoscimento del principio del *freedom of contract* come uno dei principi generali del diritto UE, v. già l'opinione dell'A.G. Kokott nella causa CGUE C-441/07 *European Commission v Alrosa Co Ltd* (par. 225), e la sentenza della CGUE del 18.7.2013 nella causa C-426/11 Alemo-Herron e altri (par. 32). Pertinente appare anche il richiamo alle c.d. esigenze imperative (c.d. rule of reason), elaborate per la prima volta dalla CGUE nella sentenza Cassis de Dijon del 1979 (Caso 120/78), in quanto costitutive di limiti all'esercizio delle libertà fondamentali dell'Unione. Per la Commissione europea, v. già il *First Annual Progress Report on European Contract Law and the Acquis Review* COM(2005) 456 final, par. 2.6.3, nonché il Considerando 30 della proposta CESL (la proposta, poi ritirata, di Regolamento del Parlamento europeo e del Consiglio relativo a un diritto comune europeo della vendita) dove si trovava dichiarato "La libertà contrattuale dovrebbe essere il principio ispiratore del diritto comune europeo della vendita. L'autonomia delle parti andrebbe limitata solo se e in quanto indispensabile, in particolare per motivi di tutela del consumatore. Qualora ricorra simile necessità, dovrebbe essere chiaramente indi-



ISSN 2239-8570

Il governo europeo della *data economy*, offre invece, a mio avviso, un piano di applicazione ideale per costruire una teoria dell'autonomia privata di diritto europeo intorno ai divieti. Tale governo, come detto, consiste oggi nelle discipline dei numerosi atti e rapporti negoziali di condivisione dei dati previsti dalle fonti UE, che prima ricordavo (DCD, direttiva *Omnibus*, DGA, Data Act, DSA), le quali ribadiscono la prevalenza del GDPR, ma alla cui considerazione vanno aggiunti i numerosi limiti all'industria dei dati che derivano anche da tutte le altre disposizioni imperative del diritto dell'Unione e nazionale. Una loro interpretazione sistematicamente coerente è, prima che urgente, doverosa. Il piano dell'atto di autonomia privata è senz'altro idoneo ad accogliere e sviluppare, in un quadro concettuale ordinato e conosciuto, un'analisi tecnico-giuridica che possa corrispondere a questo dovere ermeneutico.

cata la natura imperativa delle norme in questione". Cfr. anche l'art. 1:102 dei PECL (Principles of European Contract Law). Nel senso dell'edificazione di categorie e concetti di diritto unitario, muovendo dai problemi sottesi all'art. 82 GDPR, cfr. anche le osservazioni di C. CAMARDI, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, in *Nuova giur. civ. comm.*, 2023, 1136 e U. SALANITRO, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di Giustizia*, in *Riv. dir. civ.*, 2023, 426.



ISSN 2239-8570