PER UN SINDACATO DI LICEITÀ DEL CONSENSO *PRIVACY**

Di Salvatore Orlando

SOMMARIO*: 1. Introduzione. – 2. La socialità. La metafora dell'invito a pranzo. – 3. I diritti fondamentali. – 4. Gli interessi. L'esempio della Sig.ra Delucca, appassionata d'arte – 5. La liceità. L'esempio del Sig. Leon, impulsivo e di basso reddito. – 6. Conclusioni e aperture.*

ABSTRACT. Al fine di individuare una base adeguata allo studio e al governo del fenomeno della c.d. monetizzazione dei dati personali, l'a. esamina la disciplina del GDPR sul c.d. consenso privacy promuovendone una lettura funzionale. L'a. intende dimostrare che una simile prospettiva – che presuppone l'abbandono della concezione meramente autorizzatoria del consenso privacy, in favore di una sua qualificazione in termini di atto di autonomia privata, più aderente al vasto sistema dell'erigendo diritto europeo dei dati – non solo non comporta un pericolo per i diritti fondamentali dell'interessato, ma, al contrario, consente una loro più efficace protezione. In particolare, l'a. argomenta che la prospettiva funzionale consente e impone di vedere le ragioni tipiche degli interessati e quelle di favore del legislatore verso certe finalità del trattamento dei dati personali (funzioni lecite), e, al contempo, di disegnare i limiti dell'area dell'autonomia privata in termini di reazione giuridica a finalità lesive di diritti fondamentali e di interessi super-individuali, ossia della collettività (funzioni illecite). La prospettiva funzionale, osserva l'a., sembra ulteriormente necessaria nel quadro dell'erigendo diritto europeo dei dati, nel quale si delinea ormai con nettezza un divieto di uso dei dati personali con finalità o effetti distorsivi del comportamento delle persone e con finalità o effetti discriminatori.

With the aim of identifying a theoretical basis for the study and the governance of the phenomenon of the so-called monetization of personal data, the a. examines the GDPR legal provisions relevant to the so-called privacy consent, and promotes a purpose-oriented reading of the same. The a. seeks to demonstrate that a purpose-oriented approach – which presupposes the abandonment of the conception of the privacy consent in terms of a mere authorization, and the advent of a conception of a qualification of the same in terms of an act of private autonomy – not only is far from putting at risk the fundamental rights of the data subject, but, on the contrary, allows a more effective protection of the same, compared to the protection afforded under the approach of the privacy consent in terms of authorization. In particular, the a. argues that the purpose-oriented approach allows and requires to outline the typical rationales for the data subject and the EU legislator in favor of certain specific purposes (lawful purposes) and, at the same time, to outline the limits to the private autonomy's area in terms of contrast by the law system against certain purposes infringing fundamental rights and super-individual interests, i.e. of the community at large (unlawful purposes). The purpose-oriented approach, as the a. puts it, seems to be further necessary in the frame of the many acts (either already approved or under construction) of the new European data law, where a general prohibition clearly emerges on processing data with the purpose or the effect of distorting people's behavior, and/or with the purpose or the effect of discriminating people.

1. Introduzione.

L'obiettivo che ci proponiamo è quello di delineare alcune basi teoriche e di individuare di conseguenza alcune categorie della tecnica giuridica (strumenti) per affrontare, in termini di proposta di analisi e di trattamento giuridico, il consenso al trattamento dei dati personali (c.d. consenso *privacy*). Per avviare l'indagine, ci occuperemo del discusso fenomeno della c.d. monetizzazione dei dati personali.

Come proveremo a dire, in questo intervento (che attende naturalmente un più compiuto sviluppo, in ragione delle prospettive che suggerisce di coltivare: v. par. 6 - *Conclusioni e aperture*) proponiamo di affrontare la tematica della "monetizzazione dei dati personali"[1] promuovendo una prospettiva di analisi funzionale[2], tesa a spiegare il fenomeno sul piano degli *interessi degli interessati* (i.e. gli interessi delle persone fisiche dei cui dati personali si tratta)[3], e ad individuare al contempo un *sindacato di liceità* dell'atto in che consiste la manifestazione del consenso degli interessati al trattamento dei dati personali, inteso come atto di autonomia privata. Conformemente agli insegnamenti ricevuti con la teoria del negozio giuridico, si intuisce che il sindacato di liceità guarda, anch'esso, alla funzione del consenso, ma si situa nella dimensione degli *interessi della collettività*, ossia di interessi super-individuali, trascendenti rispetto a quelli degli stessi interessati.

Prenderemo ad oggetto di analisi immediata il fenomeno del '*tying*' nel quale l'interessato fornisce suoi dati personali non necessari per usufruire di un servizio e non paga un prezzo in denaro per usufruire del medesimo servizio[4].

---

* Il presente testo costituisce la traccia scritta, con integrazioni e note, della relazione dal titolo *La "monetizzazione" dei dati personali. Una prospettiva funzionale*, presentata dall'a. al Convegno di apertura delle celebrazioni per i 25 anni del Garante per la protezione dei dati personali, tenutosi nel Campidoglio di Roma il 24 maggio 2022, dal titolo *Il ruolo del Garante per la protezione dei dati personali: la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*. Una traccia scritta della relazione, in versione ridotta, è destinata ai relativi *Atti* per i tipi del Mulino.

[1] Seppure viene comunemente affermato che il riconoscimento normativo del fenomeno del pagamento di un bene o di un servizio attraverso dati personali si debba all'art. 3, par. 1 della direttiva (UE) 2019/770 sui contratti di fornitura di contenuto digitale e di servizi digitali, nella parte in cui fa riferimento ai contratti nei quali il consumatore fornisce o si impegna a fornire dati personali, bisogna sottolineare che del "*valore monetario*" dei dati personali in guisa di "*remunerazione*" di servizi di comunicazione elettronica, nonché della successiva "*monetizzazione*", da parte del fornitore del servizio, dei dati raccolti in conformità del GDPR, si parlava già nel Considerando 16 della direttiva (UE) 2018/1972 istitutiva del Codice europeo delle comunicazioni elettroniche: "*Per rientrare nella definizione di servizio di comunicazione elettronica, un servizio deve essere prestato normalmente dietro corresponsione di un pagamento. Nell'economia digitale i partecipanti al mercato sempre più spesso ritengono che le informazioni sugli utenti abbiano un valore monetario. I servizi di comunicazione elettronica sono spesso forniti all'utente finale non solo in cambio di denaro, ma in misura sempre maggiore e in particolare in cambio della comunicazione di dati personali o di altri dati. Il concetto di remunerazione dovrebbe pertanto ricomprendere le situazioni in cui il fornitore di un servizio chiede all'utente finale dati personali ai sensi del regolamento (UE) 2016/679 o altri dati, e questi glieli trasmette consapevolmente, per via diretta o indiretta. Esso dovrebbe ricomprendere inoltre le situazioni in cui l'utente finale autorizza l'accesso a informazioni senza trasmetterle attivamente, ad esempio i dati personali, incluso l'indirizzo IP, o altre informazioni generate automaticamente, ad esempio le informazioni raccolte e trasmesse da un cookie. Secondo la giurisprudenza della Corte di giustizia dell'Unione europea (Corte di giustizia) sull'articolo 57 TFUE, si è in presenza di remunerazione ai sensi del trattato anche se il fornitore del servizio è pagato da una terza parte e non dal destinatario del servizio. Il concetto di remunerazione dovrebbe pertanto ricomprendere anche le situazioni in cui l'utente finale è esposto a messaggi pubblicitari come condizione per l'accesso al servizio o le situazioni in cui il fornitore del servizio monetizza i dati personali raccolti in conformità del regolamento (UE) 2016/679*".

[2] Per un invito ad analizzare il fenomeno circolatorio dei dati personali, con uno sguardo alla causa del contratto, attraverso la descrizione funzionale dell'operazione economica concreta, cfr. V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 3, 2020, p. 642 ss. spec. p. 652 ss., e ora V. RICCIUTO, *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022 (su cui cfr. anche le recensioni di G. CARAPEZZA FIGLIA, *"L'equivoco della privacy". Circolazione dei dati personali e tutela della persona*, in *Jus Civile*, 2022, p. 1372 ss. e di R. SENIGAGLIA, *"L'equivoco della privacy" tra consenso e capacità*, *ivi*, p. 1378 ss.). Sulla prospettiva dell'autonomia privata e le sue interazioni con la regolazione pubblica, v. da ultimo, C. SOLINAS, *Autonomia privata e regolazione pubblica nel trattamento dei dati personali*, Bari, 2022.
Come risulterà più chiaro nel prosieguo di questa esposizione, riteniamo corretto e storicamente adeguato orientare particolarmente la prospettiva causale o funzionale facendola gravitare sulle "specifiche finalità" di trattamento dei dati personali, menzionate nell'art. 6 par. 1 lett. a) GDPR, dove (come noto) si prevede come "base" del trattamento, il "*consenso* [dell'interessato] *al trattamento dei propri dati personali per una o più specifiche finalità*".

[3] Art. 4, n. 1) Regolamento (UE) 2016/679 (GDPR): "*«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)*".

[4] Con l'espressione "*tying*" si fa riferimento all'eventualità, considerata nell'art. 7, par. 4 del 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. Questa ipotesi, che spesso ricorre in caso di servizi per i quali l'interessato non paga un prezzo in denaro (ed è allora caratteristica dei c.d. *zero price models*) si distingue da quella in cui un soggetto acquista direttamente dall'interessato il diritto di utilizzare determinati dati personali dell'interessato a fronte del pagamento di una somma di denaro, nonché dalle ipotesi della circolazione a pagamento dei dati personali successiva alla loro raccolta (sono i c.d. *personal data economy*

models). In tutti questi casi, sia pure con accenti e in modi diversi, si parla di monetizzazione o "patrimonializzazione" dei dati personali. Come noto, il Consiglio di Stato, nella famosa sentenza con la quale ha giudicato sulla sanzione a Facebook per pratica commerciale ingannevole nei confronti degli utenti, a proposito del *claim* "Facebook è gratis", ha definito i dati personali come "patrimonio di rilevante valore economico per gli operatori" (Cons. Stato, Sez. VI, 29/03/2021, n. 2631). La bibliografia è molto ampia. Dovendo limitarci in questa sede a indicazioni essenziali, si veda, anche per ulteriori riferimenti: 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, p. 417 ss; P. CARNOVALE, *La funzione sinallagmatica del trattamento dei dati personali nella fornitura di servizi digitali*, in *Giust. civ.*, n. 10/2021, p. 3 ss.; L. CASALINI, *Dati e identità personale. Note sparse a partire da una recente pronuncia del Consiglio di Stato*, in *Annuario OGID 2022- Yearbook JODI 2022*, a cura di S. Orlando e G. Capaldo, Roma, Sapienza Università Editrice, 2022, p. 53 ss.; G. D'ACQUISTO e F. PIZZETTI, *Regolamentazione dell'economia dei dati e protezione dei dati personali*, in *Analisi Giuridica dell'Economia*, 2019, p. 90 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, p. 59 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, p. 51 ss.; ID., *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Diritto dell'informazione e dell'informatica*, 4, 2020, p. 635 ss.; A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, p. 67 ss.; S. ELVY, *Paying for privacy and the personal data economy*, in *Columbia Law Review*, 2017; M. FRIES, *Data as counter-performance in B2B contracts*, in *Data as counter-performance – Contract law 2.0?* a cura di S. Lohsse, R. Schulze e D. Staudenmayer, Oxford – Baden-Baden, Hart – Nomos, 2020, p. 225 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?*, cit., p. 47 ss.; V. JANEˇCEK, G. MALGIERI, *Data extra commercium*, in *Data as counter-performance – Contract law 2.0?*, cit.,p. 95 ss.; 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, p. XI; C. LANGHANKE e M. SCHMIDT-KESSEL, *Consumer data as consideration*, in *Journal of European Consumer and Market Law*, 6, 2015, p. 218 ss.; S. LOHSSE, R. SCHULZE, D. STAUDENMAYER, *Data as counterperformance – contract law 2.0?An introduction*¸ in *Data as counter-performance – Contract law 2.0?* cit., p. 9 ss.; A. METZGER, *A market model for personal data: state of play under the new directive on digital content and digital services*, in *Data as counter-performance – Contract law 2.0?*, cit., p. 25 ss.; R. MESSINETTI, *Circolazione dei dati personali e autonomia privata*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, Cedam, 2019, p.137 ss.; Id., *Circolazione dei dati personali e autonomia privata*, in *federalismi.it*, 21, 2019, pp. 1 ss; G. MALGIERI, B. CUSTERS, *Pricing privacy the right to know the value of your personal data*, in «Computer Law & Security Review», 2017; 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, p. 35 ss. spec. p. 46 ss.; M. MURSIA M. e C.A. TROVATO, *The commodification of our digital identity: Limits on monetizing personal data in the European context*, in *MediaLaws – Rivista di diritto dei media*, n. 2/2021, p. 165 ss.; C. PERLINGIERI, *La tutela dei minori di età nei* social networks, in *Rass. dir. civ.*, 2016, p. 1324 ss.; G. RESTA, *I dati personali oggetto del contratto*, in *La circolazione dei dati*, cit., p. 55 ss.; G. RESTA e V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 436 ss.; V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., pp. 128-129; ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio e V. Ricciuto, Torino, 2019, p. 29; R. SCHULZE, *Supply of digital content. A new challenge for European contract law*, in *European contract law and the digital single market – The implications of the digital revolution*, a cura di A. De Franceschi, Cambridge, Cambridge – Antwerp – Portland, Intersentia, 2016, p. 127 ss.; I. SPEZIALE, *L'ingresso dei dati personali nella prospettiva causale dello scambio: i modelli contrattuali di circolazione*, in *Contratto e Impresa*, n. 2, 2021, p. 602; A. STAZI e F. CORRADO, *Titolarità, cessione e tutele nella circolazione dei dati*, in *La circolazione dei dati*, cit. p. 83 ss.; K. SEIN, G. SPINDLER, *The new directive on contracts for the supply of digital content and digital services – scope of application and trader's obligation to supply – Part. 1*, in *Eur. Rev. Contract Law*, 2019, p. 257 ss.; D. STAUDENMAYER, *Article 3 digital content directive (2019/770)*, in *EU Digital Law*, a cura di R. Schulze e D. Staudenmayer, München – Oxford – Baden-Baden, Beck – Hart – Nomos, 2020, p. 57 ss.; S. THOBANI, *Il pagamento attraverso dati personali*, in *Annuario OGID 2021- Yearbook JODI 2021*, a cura di S. Orlando e G. Capaldo, Roma, Sapienza Università Editrice, 2021, p. 361 ss.; ID., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, Ledizioni LediPublishing, 2018, p. 160 ss.; ID., *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws – Rivista di diritto dei media*, 3, 2019, p. 131 ss.; C.A. TROVATO, *Commercializzazione dei dati personali: limiti e condizioni*, in *Legal Tech, Big Data e contratti smart per professionisti e imprese*, a cura di S. Martinelli, C. Rossi Chauvenet, Roma, Wolters Kluwer Ipsoa, 2022; C. TWIGG-FLESNER, *Disruptive technology – disrupted law? How the digital revolution affects (contract) law*, in *European contract law and the digital single market – The implications of the digital revolution*, cit., p. 21 ss.; S. VAN ERP, *Management as ownership of data*, in *Data as counter-performance – Contract law 2.0?* cit., p. 77 ss.; F.G. VITERBO, *Freedom of contract and the commercial value of personal data*, in «Contratto e impresa Europa», 2, 2016, pp. 606-607; C. WENDEHORST, *Personal data in data value chains – is data protection law fit for the data economy?*, in *Data as counter-performance – Contract law 2.0?* cit., p. 193 ss.; H. ZECH, *Data as a tradeable commodity*, in *European contract law and the digital single market – The implications of the digital revolution*, cit., p. 51 ss.; OECD, *Quality considerations in digital zero-price markets. Background note by the Secretariat*, 2018; OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, 2013.

In adesione al canone ermeneutico della drammatizzazione dell'esito dell'interpretazione,

portato a teoria dal Maestro di Camerino[5], mireremo all'emersione esemplificativa dei concetti che intendiamo promuovere, ed adotteremo, a tal fine, non già esempi di nostra fantasia, bensì esempi fatti dal Comitato europeo per la protezione dei dati personali (EDPB), nelle sue Linee guida sul *targeting online* adottate nell'aprile 2021[6]. Quindi, esempi, per così dire, istituzionali, sui quali gli esperti di questa materia si sono già confrontati e continueranno a confrontarsi.

Prima di ciò, per preparare il terreno alla trattazione di questi esempi, diremo qualcosa sulla socialità, la storicità e i diritti fondamentali: chi legge potrà trovare ragioni per perdonare la velocità di trattazione di temi così importanti nella dichiarata loro utilizzazione al solo ed esclusivo fine di introduzione degli esempi istituzionali dell'EDPB.

2. La socialità. La metafora dell'invito a pranzo

Il campo della nostra indagine è l'ecosistema digitale, la monetizzazione dei dati personali compiendosi nell'ecosistema digitale. Come si sa, infatti, è a proposito dei *dati digitali* che si parla di economia dei dati (*data economy*)[7].

In proposito, è diffusa l'osservazione per la quale, nella materia dell'innovazione digitale, la legge deve seguire la tecnologia che cambia. Ed è vero: senza dubbio il legislatore deve stare al passo con i tempi: comprendere – prima – per regolare – poi – certi fenomeni. Ma è vero anche che quella osservazione va precisata, perché essa rischia di essere intesa in un senso limitativo. È opportuno specificare che il legislatore, essenzialmente, si deve occupare e si occupa del *riflesso che queste innovazioni hanno sui rapporti sociali*. In altre parole, il legislatore deve comprendere non solo i cambiamenti tecnologici, ma anche quelli dei rapporti sociali che ne conseguono.

Dunque in questa materia - come d'altronde in ogni materia - la legge segue anche *l'idea di socialità*, che cambia anch'essa col tempo.

La socialità è la sintesi tra i comportamenti osservati e quelli accettati all'interno di una comunità. Essi, tanto quelli osservati, quanto quelli accettati, mutano diacronicamente, ossia nel tempo. Da qui la storicità del diritto. E la storicità permea l'oggetto elettivo della nostra indagine: la 'monetizzazione dei dati personali'. Perché si tratta di una espressione che indica anche, e forse innanzitutto, lo stupore della Storia.

Per fermare all'attenzione e dimostrare, relativamente al nostro tema, la socialità che cambia e crea stupore, useremo una metafora.

Un padrone di casa mi invita «vieni domani a pranzo, ci saranno molte persone che vuoi vedere, altre che potrebbero interessarti, e, in disparte, altre ancora che mi pagano per osservarvi e sapere qualcosa di voi».

Fino a qualche anno fa, certamente, la stragrande maggioranza delle persone che avesse ricevuto un invito del genere lo avrebbe declinato, e nemmeno troppo gentilmente. Oggi un simile invito è accettato, ogni giorno, da miliardi di persone.

3. I diritti fondamentali

Di fronte a una simile constatazione, viene automatico - al giurista - cercare ricovero nei diritti fondamentali. Ma è, ad essere franchi, un percorso di analisi che, di per sé, non è idoneo a spiegare le *ragioni* del fenomeno. Può e deve - senz'altro - assistere a governarlo, però *dopo averlo compreso*.

Inoltre, il richiamo alla pur incontestabile necessità del governo del fenomeno sulla base dei diritti fondamentali, non può ignorare la doppia direzione per la quale, se è vero che il Diritto (attraverso la sua azione improntata anche e innanzitutto ai diritti fondamentali) esercita una pressione di *dover essere* sulla Società, e quindi agisce in una certa misura sulla *conformazione dei comportamenti*, è vero anche che la Società (attraverso il continuo esercizio di sintesi che la comunità governata compie nel suo seno tra i comportamenti osservati e quelli accettati dai consociati) esercita una pressione di *essere* (nel senso di esser*ci*, di effettività) sul Diritto, e quindi agisce fatalmente, in una certa misura, sulla *conformazione del Diritto* e così anche sulla

[5] Betti, *Interpretazione della legge e degli atti giuridici*, Milano, 1949, p. 5: «Inoltre l'interprete deve — come dovette già chi emanò la norma o la pronuncia di carattere precettivo — raffigurarsi nelle reazioni e ripercussioni pratiche, e in questo senso drammatizzarsi (*realize*, si direbbe in inglese), l'esito della interpretazione che sta per proporre e sostenere. Insomma, a differenza dall'interprete che ha in vista un esito puramente conoscitivo, l'interprete qui ha in vista, attraverso il risultato intellettivo, un esito pratico, che conduce a prender posizione in date situazioni ipotizzate in anticipo».

[6] EDPB, *Linee guida 8/2020 sul* targeting *degli utenti di social media*, versione 2.0, adottate il 13 aprile 2021: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_it

[7] Cfr. *European Commission, European Data Market study* (SMART 2013/0063), IDC, 2016; *Updated European Data Market (EDM) study* (SMART 2016/0063), 2020; *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, "Costruire un'economia dei dati europea"*, COM/2017/09 *final*.

conformazione degli stessi diritti fondamentali (*Sinngebung*)[8].

È d'altronde indiscutibile che tutte le domande che possiamo proporci così come tutte le risposte che possiamo fornire a proposito dei diritti fondamentali sono *storicamente condizionate*.

Dunque dobbiamo prendere atto che nel nostro discorso non c'è possibilità di ricovero *dalla* Storia. Si tratterà pertanto – per cominciare – di provare a capire il fenomeno, procedendo – come sempre si fa – dagli interessi.

4. Gli interessi. L'esempio della Sig.ra Delucca, appassionata d'arte

Secondo l'impostazione comunemente fruita, quell'invito a pranzo si scompone – fuor di metafora – in una offerta di servizio senza pagare un prezzo in denaro e in una richiesta di consentire al *tying* ossia alla raccolta e trattamento di dati personali.

La domanda che attende una risposta è: *perché miliardi di persone acconsentono ogni giorno al tying?* Seguendo l'impostazione tradizionale che affronta la questione sotto l'angolo visuale della libertà del consenso (mi riferisco alle Linee guida EDPB 5/2020 sul consenso e alla nota sentenza Cass. 17278/2018[9]) bisognerebbe concludere che il consenso al *tying* o è invalido oppure è inspiegabile.

Ed effettivamente, sulla scorta della soluzione ermeneutica che fa leva sulla fungibilità o equivalenza del servizio per giudicare sulla libertà del consenso[10], bisognerebbe dire che il consenso al

[8] L. MENGONI, *Ermeneutica e dogmatica giuridica: saggi*, Milano, Giuffré, 1996.

[9] Questa impostazione, come noto, si è sviluppata intorno alla previsione contenuta nell'art. 7, par. 4 GDPR secondo cui: «*[n]el valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, 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*». Su tale base, lo *European Data Protection Board* ha affermato che il consenso non può essere considerato libero quando è "*condizionato*", cioè quando "*la fornitura di un contratto o servizio [è subordinata] a una richiesta di consenso al trattamento di dati personali che non sono necessari per l'esecuzione del contratto o servizio*". Affinché il consenso sia libero è necessario che il titolare del trattamento permetta all'interessato "*di scegliere tra un servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente che non implica un siffatto consenso, dall'altro. Finché esiste la possibilità che il contratto venga eseguito o che il servizio oggetto del contratto venga prestato dal titolare del trattamento senza necessità di acconsentire ad usi ulteriori o supplementari dei dati in questione non si è in presenza di un servizio condizionato. Tuttavia, i due servizi devono essere effettivamente equivalenti*": EDPB, *Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679*, punto 25 ss., spec. punto 37. Anche la Corte di Cassazione è intervenuta sul tema dichiarando che è lecito subordinare l'accesso a un bene o servizio alla prestazione del consenso al trattamento solo se il bene o il servizio è "*fungibile*", per cui l'interessato ha la possibilità di accedere a servizi o beni analoghi senza dover prestare il proprio consenso. Al contrario, subordinare l'accesso a un bene o servizio alla prestazione del consenso al trattamento è vietato se la prestazione è "*ad un tempo infungibile ed irrinunciabile per l'interessato*" (Cass. 17278/2018).

[10] Sul consenso, senza pretesa di completezza, cfr. A. ASTONE, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle* cose, Milano, 2019; ID., *L'accesso dei minori di età ai servizi della c.d. società* dell'informazione, in *Contr. impr.*, 2019, p. 614 ss.; L. AULINO, *Consenso al trattamento dei dati e carenza di consapevolezza: il legal design come un rimedio* ex ante, *in Dir. inf.*, 2020, p. 303 ss.; C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità al trattamento dei dati personali,* in *Contr. impr.*, 2020, p. 860 ss.; L. BOZZI, *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, in *Europa e dir. priv.*, 2020, p. 251 ss.; F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento*, in *Il nuovo regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, diretto da G. Finocchiaro, Bologna, 2017, p. 138 ss.; ID., *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. impr.*, 1/2019, p. 34 ss.; F. CAGGIA, *Il diritto ai trattamenti dei dati personali nel diritto europeo*, in *Riv. dir. comm.*, 2019, p. 405 ss.; I.A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo regolamento europeo*, in *Oss. Dir. civ. comm.*, 2018, p. 67 ss.; ID., *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del regolamento UE 2016/679, tra diritto e tecnoregolazione*, in *Familia*, 2018, p. 3 ss.; V. CARBONE, *Il consenso, anzi i consensi, nel trattamento informatico dei dati personali*, in *Danno resp.*, 1998, p. 23 ss.; V. CUFFARO, *Il consenso* dell'interessato, in *La disciplina del trattamento dei dati personali*, a cura di V. Cuffaro e V. Ricciuto, Torino, 1997, p. 201 ss.; A.M. GAROFALO, *Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR*, in *Annuario OGID 2021- Yearbook JODI 2021*, cit., p. 119 ss.; ID., *Cookies and the Passive Role of the Data Subject*, in *Privacy and Data Protection in Software Services*, cit., p. 77 ss.; L. GATT, R. MONTANARI, I.A. CAGGIANO, *Consent to the processing of personal data: a legal and behavioural analysis. Some Insights into the Effectiveness of Data Protection Law*, in EJPLT, 2018, p. 1-15; IIDD., *Consenso al trattamento dei dati personali e analisi giuridico comportamentale. Spunti di una riflessione sull'effettività della tutela dei dati personali*, in *Pol. Dir.*, 2017, p. 363 ss.; S.F. GIOVANNANGELI, *L'informativa agli interessati e il consenso al trattamento*, in *Libera circolazione e protezione dei dati personali* a cura di R. Panetta, Milano, 2019, p. 99 ss.; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021; P. MANES, *Il consenso al trattamento dei dati personali*, Padova, 2001; S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in *Libera circolazione e protezione dei dati personali*, cit., I, p. 993 ss.; D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, p. 339 ss.; R. MESSINETTI, *Circolazione dei dati personali e autonomia privata*, cit., p. 142 ss.; F. NADDEO, *Il consenso al trattamento dei dati personali del minore*, in *Dir. inf.*, 2018, p. 27 ss.; G. OPPO, *Sul consenso dell'interessato,* in *Trattamento dei dati e tutela della persona* a cura di V. Cuffaro, V. Ricciuto e V. Zeno-Zencovich, Milano, 1998, p. 123 ss.; D. POLETTI, *IoT and*

tying o si spiega (i.e. si acconsente al *tying* per accedere ad un servizio senza pagare in denaro) ma è invalido (perché, secondo quella impostazione, il consenso non è libero) oppure è valido (perché, secondo quella impostazione, è libero) ma è inspiegabile. Ed infatti, perché mai – di fronte a eventuali casi concreti di servizi alternativi fungibili o equivalenti, prestati dallo stesso fornitore o da altri, che non richiedono né un pagamento in denaro né il *tying* – dovrebbe prestarsi il consenso al *tying*?

Dobbiamo perciò ammettere che, impostata in questi termini la questione, essa si muove in un vicolo cieco; che, obiettivamente, non ci consente di spiegare plausibilmente il fenomeno.

Per rispondere alla domanda sul *perché*, ossia *quale interesse* possano avere gli interessati a prestare il consenso al *tying*, bisogna avere il coraggio di scartare la risposta che sembra ovvia, ma che, come visto, non aiuta (ossia bisogna scartare la spiegazione per la quale l'interesse consisterebbe esclusivamente nel non pagare un prezzo in denaro per ricevere un servizio) e bisogna cominciare col guardare le finalità del trattamento.

E bisogna avere, inoltre, l'avvedutezza di scartare l'ipotesi (e l'obiezione implicitamente in essa contenuta che indirizza la domanda verso una risposta necessariamente negativa) che possa trattarsi di un generico 'interesse a ricevere pubblicità'. Riferirsi in questo contesto semplicemente alla pubblicità tradizionalmente considerata, sarebbe sbagliato in quanto tradirebbe una conoscenza del fenomeno limitata e ampiamente superata dalla realtà del mondo del *marketing* contemporaneo.

Se - anche qui - storicizziamo, a quella domanda possiamo rispondere affermando che non si tratta di un generico interesse a ricevere pubblicità, bensì di un interesse alla *comunicazione personalizzata* e ai *contenuti digitali*, ossia che si tratta di un interesse a trovare, a rimanere dentro, o a non essere esclusi da, *il proprio posto nell'ecosistema digitale.*

Per supportare queste affermazioni, nei limiti del presente intervento, sarà sufficiente ricordare, in breve, i passaggi che dalla pubblicità tradizionale ci hanno condotto oggi alla *comunicazione*.

Dalla pubblicità commerciale tradizionale, diretta ad influenzare la scelta di acquisto di prodotti, si è passati ad avere contezza - anche da parte del legislatore - della maggiore ampiezza del *marketing* rispetto alla pubblicità, come insieme di tecniche e procedure orientate ad influenzare qualunque comportamento, non solo l'acquisto di un prodotto. E così, in ambito commerciale, anche gli atti di esercizio di diritti contrattuali, l'attivazione di garanzie, l'esercizio del diritto di recesso, l'esercizio e la scelta di certe facoltà e diritti nella fase c.d. post-vendita, etc.

È anche risaputo che il *marketing* commerciale non si esaurisce in quello consumeristico, c'è anche un *marketing* B2B.

Ed è infine ben noto che il *marketing* non si esaurisce nella sfera commerciale: come è noto a tutti, esiste un *marketing* non-commerciale, ad esempio il *marketing* politico inteso ad influenzare il voto o l'associazione a partiti o movimenti politici, il *marketing* delle associazioni di beneficienza finalizzato a creare associati, alla raccolta di fondi, delle Chiese e associazioni religiose, il *marketing* sociale[11] etc.[12]

È del 25 novembre 2021 la proposta di Regolamento avanzata dalla Commissione europea per disciplinare il *marketing* politico e la c.d. amplificazione.[13]

Ma ciò che consente di rispondere direttamente alla domanda che ci siamo proposti è la constatazione che il *marketing* ormai è sinonimo di

Privacy, in *Privacy and Data Protection in Software Services*, cit., p. 175 ss.; G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2000, p. 299 ss.; G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 411 ss.; A. SATTLER, *Autonomy or heteronomy – Proposal for a two-tier interpretation of Article 6 GDPR*, in *Data as counter-performance – contract law 2.0?*, cit. p. 225 ss.; M. SCHMIDT-KESSEL, *Consent for the processing of personal data and its relationship to contract*, in Digital revolution – New challenges for law a cura di A. De Franceschi e R. Schulze. Oxford – Baden-Baden, Beck – Nomos, 2019, p. 75 ss.; S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, 2001, p. 621 ss.; S. THOBANI, *Il consenso al trattamento dei dati personali*, in *Manuale di diritto privato delle nuove tecnologie*, cit., p. 133 ss.; ID., *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Media Laws*, 2019, pp. 131 ss.; ID., *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, 2016; ID., *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa e dir. priv.*, 2016, p. 513 ss.; A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale*, Napoli, 2019; V. ZENO-ZENCOVICH, *Il "consenso informato" e la "autodeterminazione informativa" nella prima decisione del Garante*, in *Corr. Giur.*, 1997, pp. 915 ss.

[11] Il concetto di "marketing sociale" è stato introdotto nel 1971 da Philip Kotler per indicare l'utilizzo delle strategie e delle tecniche del marketing per influenzare un gruppo target ad accettare, modificare o abbandonare un comportamento in modo volontario, al fine di ottenere un vantaggio per i singoli individui o la società nel suo complesso. Cfr. P. KOTLER e G. ZALTMAN, *Social marketing: an approach to planned social change*, in *Journal of Marketing*, 35, 1971, pp. 3-12.

[12] P. KOTLER, K. KELLER, *Marketing management*, 12 ed. a cura di W. G. Scott, trad. it. di F. Sarpi, Milano 2007, p. 7; P. KOTLER, J. ARMSTRONG, V. WONG, J. SAUNDERS, *Principles of marketing*, 5^ ed, Londra (Pearson), 2008, p. 32 ss., p. 623 ss.

[13] COM(2021) 731 *final.*

comunicazione: i *marketer* disegnano strategie di *marketing* su stili di vita, abitudini e credenze delle persone (credenze storiche, religiose, politiche) in quanto indirettamente funzionali al comportamento che vogliono influenzare, alla risposta che vogliono ottenere.

Oggi il vecchio CAP (Codice di autodisciplina pubblicitaria) si chiama "Codice di autodisciplina della *comunicazione* commerciale" e c'è una sezione per la "comunicazione sociale". Per i *target* (bersagli) delle campagne di *marketing* si costruiscono 'esperienze', informazioni e contenuti personalizzati**.**

Tornando più da vicino alle nostre questioni, le già citate Linee guida dell'EDPB n. 8/2020 sul *targeting* degli utenti di *social media*, contengono in sequenza due esempi - il n. 7 e il n. 8 - che ci sembrano significativi per il discorso che andiamo svolgendo. Ricordiamo qui di seguito l'esempio n. 7 e nel prossimo paragrafo ricorderemo l'esempio n. 8.

L'esempio n. 7 delle Linee Guida EDPB 8/2020 è quello della Sig.ra Delucca, un'appassionata di pittura impressionista [14]. In questo esempio, la signora Delucca, dopo aver messo più volte "mi piace" alle foto postate dalla galleria d'arte di un pittore impressionista sulla pagina di una piattaforma *social*, riceve da un museo la pubblicità di una mostra di pittori impressionisti. Il museo sta infatti cercando di attirare persone interessate a dipinti impressionisti in vista di una sua prossima mostra e, per fare ciò, utilizza una serie di criteri di *targeting* offerti dal fornitore di *social media* che caratterizzano il profilo di "*persona interessata all'impressionismo*". In questo caso, è facilmente intuibile come la signora Delucca possa avere un genuino interesse a ricevere tale tipo di comunicazione in quanto le offre la possibilità di visitare la mostra di un pittore potenzialmente in linea con i suoi gusti artistici, con ciò che ne può conseguire anche in termini di conoscenza di nuove opere e di contatti di persone e organizzazioni che hanno interessi o operano professionalmente nel campo della pittura con specializzazione nella corrente impressionista. Senza una profilazione e un *targeting* basati sul trattamento dei suoi dati personali attraverso l'algoritmo finalizzato al tracciamento e al bersaglio del profilo di "*persona interessata all'impressionismo*", la Sig.ra Delucca con tutta probabilità non sarebbe venuta a conoscenza di quella mostra, e sicuramente non ne sarebbe venuta a conoscenza così rapidamente e senza bisogno di impiegare tempo per fare ricerche.

[14] EDPB, *Linee guida 8/2020 sul* targeting *degli utenti di social media*, versione 2.0, adottate il 13 aprile 2021, punto 80 (p. 27).

Questo esempio ci fa comprendere come può esserci un interesse dell'interessato dietro l'informazione personalizzata, e che si tratta di un interesse meritevole di tutela. Essendo indiscutibile che esistano interessi commerciali anche in coloro che procedono ad un siffatto trattamento dei dati personali della Signora Delucca (profilazione e *targeting*), questo esempio ci fa comprendere come il consenso al *tying* possa perseguire in questo specifico caso[15], considerando tutti i soggetti in gioco, *interessi meritevoli di tutela*.

5. La liceità. L'esempio del Sig. Leon, impulsivo e di basso reddito

Nella metafora dell'invito a pranzo, l'esempio sopra riferito della Signora Delucca, appassionata d'arte, che viene a conoscenza di una mostra di pittura impressionista, riguarda le "persone che potrebbero interessarti". Esse sono individuate attraverso la profilazione[16] dell'invitato e la conseguente *personalizzazione* della comunicazione.

Per questo motivo, abbiamo detto che l'interesse a ricevere informazioni personalizzate equivale oggi all'interesse a essere inclusi nella, e a non essere esclusi dalla, dimensione della comunicazione digitale.

In questo senso, dobbiamo anche riconoscere che il consenso al *tying* è indubbiamente una strada molto facile per rimanere dentro l'ecosistema digitale. E che, *di per sé*, si tratta di un interesse meritevole di tutela.

Il problema oggi, semmai, è che *è la strada più facile*. Ed è un problema, in quanto questa situazione di fatto può comportare abusi.

Si viene così al tema della liceità.

Anche qui, dobbiamo limitarci ad alcuni cenni sintetici.

L'economia di massa del XX secolo era *spersonalizzante*: tutti numeri, tutti uguali[17]. Ma in questa solitudine (la solitudine dei numeri tutti) c'era, se vogliamo, il massimo della *privacy*.

[15] Ossia, per la specifica e granulare finalità di profilazione, non genericamente intesa, bensì analiticamente individuata dall'algoritmo di "persona interessata all'impressionismo".

[16] Sulla profilazione cfr. R. MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, in *Persona e mercato dei dati. Riflessioni sul* GDPR, a cura di N. Zorzi Galgano, Milano, Wolters Kluwer – Cedam, 2019, p. 167 ss.

[17] Si parla di "*marketing* di massa" o "*macromarketing*" per indicare un modello volto a creare strategie di marketing rivolte al pubblico più ampio possibile e senza badare ai parametri di segmentazione del mercato. G. JONES E R.S. TEDLOW, *The Rise and Fall of Mass Marketing*, London, Routledge, 1993.

Nei primi venti anni del XXI secolo l'economia e la comunicazione sono diventate sempre più *personalizzate*. Abbiamo visto che il *marketing online* è oggi in larga parte personalizzato.

Il rischio che si fronteggia oggi è che l'economia e la comunicazione divengano *personalizzanti*[18].

I teorici e gli strateghi del *marketing* osservano che nell'era dell'informazione digitale "*i marketer devono trasformarsi da cacciatori a giardinieri*"[19], sottolineano "*l'importanza della continuità del presidio social per la comprensione dei comportamenti e lo stimolo all'engagement degli utenti*" e notano che nel loro lavoro è fondamentale il fattore tempo, la "*pazienza*" e la "*prontezza nel cogliere le opportunità*"[20].

Per questo motivo, i *marketer* disegnano strategie che impiegano i *social*, per comunicare stili di vita, abitudini e perfino credenze (come sopra ricordato in breve) in quanto indirettamente funzionali al comportamento che vogliono influenzare, alla risposta che vogliono ottenere; e i primi target delle campagne di *marketing* sono i bambini, dai 4 anni in su.

In questo contesto, i rischi sono quelli della *distorsione comportamentale* e della *discriminazione*: le persone il cui comportamento viene, non semplicemente influenzato, bensì, distorto[21] ossia manipolato, attraverso una comunicazione personalizzata che fa leva su loro specifiche e ben studiate caratteristiche e vulnerabilità decisionali e comportamentali, *rischiano tipicamente di diventare persone diverse* da quelle che sarebbero diventate se non fossero state fatte bersaglio di quella comunicazione.

Questo è quello che si intende dire quando si parla di contrasto alle pratiche di sfruttamento della vulnerabilità, nonché a pratiche di radicalizzazione, polarizzazione o amplificazione. E, si badi, ciò vale anche per la discriminazione, perché vi è una capacità personalizzante anche nelle pratiche discriminatorie: si spingono le persone discriminate a comportarsi come tali.

È bene sottolineare che non si tratta di un'analisi di rischi di natura sociologica. Al contrario, sono rischi tutti ben presenti al legislatore europeo, che li ha messi al centro di *precisi divieti*, specificati e confermati nel sorgente diritto europeo dei dati.

Per il rischio di distorsione comportamentale vengono in conto, *inter alia*: il divieto generale delle pratiche commerciali distorsive del comportamento economico dei consumatori (art. 5 Dir. 2005/29/CE); i divieti di immissione sul mercato, messa in servizio e uso di sistemi di IA distorsivi del comportamento (anche non economico) delle persone (anche non consumatori) (art. 5 lett. *a)* e *b)* Proposta di Artificial Intelligence Act 'AIA' COM(2021) 206 *final*); il divieto di tecniche di *targeting* o amplificazione in ambito di pubblicità politica che comportano il trattamento dei dati personali di cui all'art. 9.1 GDPR (art. 12 Proposta di regolamento sulla trasparenza e *targeting* della pubblicità politica COM(2021) 731 *final*); il divieto di tecniche di *targeting* o amplificazione che comportano il trattamento, la rivelazione o la deduzione di dati personali di minori o dati personali di cui all'art. 9.1 GDPR per finalità pubblicitarie (art. 26, par. 3 del *Digital Services Act* 'DSA'[22]). Per il rischio di discriminazione, viene in conto, *inter alia*, il divieto di uso da parte di pubbliche autorità di sistemi di IA di *social scoring* discriminatorio (art. 5, lettera *c)* Proposta AIA).

In questo contesto, viene in evidenza il trattamento di speciali categorie di dati, che

[18] Cfr. le perspicue osservazioni di R. MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, cit., p. 167 ss., spec. p. 188 ss. dove l'a. parla del "*processo di costruzione dell'identità*" attraverso le profilazioni e di una sostituzione della libertà dell'autodeterminazione dell'individuo con la "*efficienza dell'eterodeterminazione informatizzata*".

[19] M.S. SAWHNEY e P. KOTLER, *Marketing in the Age of Information Democracy* in *Kellogg on Marketing*, John Wiley & Sons, 2001, pp. 386-408.

[20] Così si legge nella *Prefazione* di S. A*ddamiano* alla edizione italiana di P. KOTLER, S. HOLLENSEN, M.O. OPRESNIK, *Social media marketing, Marketer nella rivoluzione digitale*, Milano, Hoepli, 2019, pp. XIV – XV.

[21] La differenza tra influenza comportamentale (ammessa in linea di principio in quanto esercitata in conformità alla 'diligenza professionale') e distorsione comportamentale (vietata, in quanto conseguenza di pratiche contrarie alla 'diligenza professionale') è stata tracciata con il divieto delle pratiche commerciali sleali, dalla direttiva 2005/29/CE.

[22] Art. 26, par. 3 del Regolamento (UE) 2022/2065 del 19 ottobre2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE: "*I fornitori di piattaforme online non possono presentare pubblicità ai destinatari del servizio basate sulla profilazione, quale definita all'articolo 4, punto 4), del [GDPR], utilizzando le categorie speciali di dati personali di cui all'articolo 9, paragrafo 1, del regolamento[GDPR]*".
E ricordiamo come già nel 2005 il Garante italiano per la protezione dei dati personali, presieduto da Stefano Rodotà, avesse adottato una decisione dal tenore simile, a proposito della questione delle carte fedeltà ('*Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione - 24 febbraio 2005 [1103045]*: Punto 2 "[…] *Come premesso, l´utilizzazione di dati sensibili (art. 4, comma 1, lett. d), del Codice) non è di regola ammessa per alcuna delle finalità indicate, fatta salva l´ipotesi eccezionale nella quale il trattamento di dati sia realmente indispensabile in rapporto allo specifico bene o servizio richiesto e sia stato autorizzato dal Garante, oltre che acconsentito per iscritto dall´interessato. Ciò, vale anche per eventuali ricerche di mercato, sondaggi ed altre ricerche campionarie (cfr. aut. gen. Del Garante n. 5/2004, in G.U. 14 agosto 2004, n. 190)* […]").

consente lo sfruttamento di vulnerabilità decisionali e comportamentali.

Come sintetizzato nel Considerando 69 del medesimo DSA: "*Quando ai destinatari del servizio vengono presentate inserzioni pubblicitarie basate su tecniche di targeting ottimizzate per soddisfare i loro interessi e potenzialmente attirare le loro vulnerabilità, ciò può avere effetti negativi particolarmente gravi. In alcuni casi, le tecniche di manipolazione possono avere un impatto negativo su interi gruppi e amplificare i danni per la società, ad esempio contribuendo a campagne di disinformazione o discriminando determinati gruppi. Le piattaforme online sono ambienti particolarmente sensibili per tali pratiche e presentano un rischio per la società più elevato. Di conseguenza, i fornitori di piattaforme online non dovrebbero presentare inserzioni pubblicitarie basate sulla profilazione, come definite all'articolo 4, punto 4), del [GDPR], utilizzando le categorie*

speciali di dati personali di cui all'articolo 9, paragrafo 1, dello stesso regolamento, anche utilizzando categorie di profilazione basate su tali categorie speciali. Tale divieto lascia impregiudicati gli obblighi applicabili ai fornitori di piattaforme online o a qualsiasi altro fornitore di servizi o inserzionista coinvolti nella diffusione della pubblicità a norma del diritto dell'Unione in materia di protezione dei dati personali".

In altre parole, al legislatore europeo è ben presente che la comunicazione personalizzata, se da un lato offre il vantaggio di orientare la navigazione delle persone nel, pressocché sterminato, *mare magnum* delle informazioni in formato digitale (disponibili in tutte le lingue e su praticamente ogni argomento), dall'altro lato comporta innegabili rischi di abuso, in particolare nelle forme della distorsione comportamentale e della discriminazione [23].

Una efficace raffigurazione di questi rischi è data dalle Linee guida dello EDPB sopra citate, dove, nell'esempio 8, si legge: «*Il signor Leon ha indicato nella propria pagina di social media di essere interessato allo sport […]. Visita […] siti web di gioco d'azzardo online. Il fornitore di social media traccia l'attività online del signor Leon sui suoi molteplici dispositivi […]. 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 […] 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 […]*»[24].

La profilazione realizzata – in questo esempio 'istituzionale' - nei confronti del Sig. Leon, seppur a prima vista potrebbe apparire simile a quella illustrata nell'esempio immediatamente precedente della signora Delucca, in realtà presenta una significativa differenza. Infatti, nel caso della Signora Delucca la profilazione avviene sulla base di un criterio e per una specifica finalità di *targeting* – l'interesse per la pittura impressionista – che non denota una situazione di vulnerabilità ed è finalizzata all'invio di comunicazioni personalizzate a vantaggio della stessa interessata (che nel caso di specie viene a conoscenza di una mostra di suo interesse). Al contrario, l'esempio del Sig. Leon mostra una profilazione basata su criteri di *targeting* – quali il carattere impulsivo e il basso reddito – che vengono utilizzati per individuare soggetti specificamente vulnerabili sotto due aspetti (caratteriale e reddituale) che, proprio in ragione delle loro specifiche e ben studiate vulnerabilità, potranno essere manipolati. Mentre dunque nel primo caso c'è un interesse meritevole di tutela a che la signora Delucca acconsenta a essere profilata e a ricevere quel tipo di comunicazioni, nel secondo caso non può essere ammesso che il Sig. Leon venga assoggettato, sia pure con il suo consenso esplicito, a una simile pratica persecutoria, specificamente intesa a sfruttare sue precise vulnerabilità decisionali e comportamentali.

E tuttavia, è questa la conclusione che, ad oggi, l'EDPB indica a proposito di questo esempio. Ed infatti, in quelle Linee Guida si legge che il Sig. Leon con il suo consenso esplicito ex art. 22 GDPR, può acconsentire alla presentazione mirata di pubblicità (*targeting*) di scommesse *online*, sulla base di simili algoritmi di profilazione.[25] Ossia che con il suo consenso esplicito il Sig. Leon potrebbe essere fatto legittimamente bersaglio di pratiche di

[23] Cfr. R. MONTINARO, *I sistemi di raccomandazione nelle interazioni tra professionisti e consumatori: il punto di vista del diritto dei consumi (e non solo)*, in *Persona e mercato*, 3/2022, p. 368 ss.

[24] EDPB, *Linee guida 8/2020 sul* targeting *degli utenti di social media*, cit., punto 80.

[25] EDPB, *Linee guida 8/2020 sul* targeting *degli utenti di social media*, cit., punto 88: "*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*".

sfruttamento della sua vulnerabilità decisionale, vale a dire di pratiche di distorsione comportamentale.

Il consenso appunto.

Senza girarci intorno, riteniamo che sia necessario affermare un'interpretazione degli artt. 6, 9 e 22[26] del GDPR adeguata e coerente con la consapevolezza espressa, e con le norme di contrasto dei suesposti rischi di distorsione comportamentale e di discriminazione messe in campo dal legislatore europeo nel sorgente diritto europeo dei dati. In particolare, quanto all'art. 6.1 lett. *a)* del GDPR, riteniamo che esso debba interpretarsi nel senso che sottintenda necessariamente l'aggettivo "legittime" quando parla di «*specifiche finalità*»; come d'altronde la successiva lettera *b)* deve interpretarsi nel senso che esso sottintenda necessariamente l'aggettivo "lecito" quando parla di «*contratto*», perché non può ritenersi che la base del trattamento possa essere l'esecuzione di un contrato illecito.

Allo stesso modo – dunque - deve ritenersi che non possa essere valido il consenso come base di trattamento se è rivolto a specifiche finalità illegittime.

D'altronde, nessuno dubita, ed anzi è ribadito continuamente nelle linee guida, che i principî dell'art. 5 GDPR si applichino sempre, anche in costanza di dati personali trattati sulla base del consenso. Si ricorda in proposito che l'art. 5.1 *a)* GDPR impone la liceità e la correttezza del trattamento, e l'art. 5.1 *b)* GDPR, relativamente al principio di limitazione, impone che i dati personali siano raccolti per finalità legittime.

Se questo è sicuro, va contrastata e superata la concezione circolare e formalistica per il quale il trattamento è lecito se ricorre la base del consenso, senza guardare altro che i requisiti di libertà, specificità, informazione ed inequivocabilità del consenso, ossia senza guardare alla funzione per la quale il consenso è prestato.

La base del consenso sub art. 6.1 *a)* non può essere il semplice consenso, sia pure libero, specifico, informato ed inequivocabile, perché un simile consenso potrebbe essere reso per qualsiasi finalità di trattamento, anche illegittima: deve essere invece un consenso siffatto (ossia libero, specifico, informato ed inequivocabile) reso per specifiche finalità di trattamento legittime.

Dunque una giustificazione funzionale deve esserci, come a ben vedere c'è, per *tutte* le basi ex art. 6 GDPR.

Piuttosto, ma qua possiamo solo accennare alla questione, va promossa, insieme all'idea del requisito della granularità del consenso, l'idea della 'granularità delle finalità' e affermare che solo alcune finalità sono ammesse dall'ordinamento in quanto legittime: non basta dire "finalità di profilazione", "finalità di *marketing*", "finalità di *targeting*". Queste non sono "specifiche" finalità di trattamento. Come ci insegnano i due esempi della Sig.ra Delucca e del Sig. Leon, fatti nelle citate Linee Guida dell'EDPB, ci sono algoritmi che lavorano per finalità specifiche. Bisogna dunque analizzare nello specifico gli algoritmi[27] di creazione e bersaglio dei profili per stabilire la legittimità delle specifiche finalità di trattamento. E bisogna distinguere quelli che perseguono finalità legittime da quelli che perseguono finalità illegittime, perché - come nell'esempio del Sig. Leon – esistono e sono molto diffusi algoritmi disegnati esattamente per sfruttare vulnerabilità decisionali e comportamentali.

Non possiamo soffermarci in questa sede sulla *struttura* del consenso a partire dalle diverse e non perfettamente sovrapponibili versioni delle diverse lingue ufficiali del GDPR dedicate alla definizione di consenso di cui all'art. 4 n. 11 GDPR.

Qui è sufficiente osservare che anche nella versione italiana non c'è dubbio alcuno che si tratti di una manifestazione di volontà libera rivolta a un fine, dunque che si tratta di un *atto di autonomia*.

Come atto di volontà libera rivolto a un fine, naturalmente, c'è un *controllo della sua funzione* – ossia del suo fine – da parte della legge: tanto più oggi che si parla di monetizzazione e di condivisione di dati per le più varie finalità (tra cui l'altruismo dei dati), e si prevedono servizi di intermediazione per fini commerciali, e cooperative.

[26] Cfr. da ultimo, anche per riferimenti bibliografici, D. IMBRUGLIA, *Diritti fondamentali e ambienti digitali: prime note di una ricerca sul diritto a non essere sottoposto a una decisione interamente automatizzata*, in *Annuario OGID 2022-Yearbook JODI 2022*, a cura di S. Orlando e G. Capaldo, Roma, Sapienza Università Editrice, 2022, p. 113 ss; e anche L. EDWARDS, M. VEALE, *Enslaving the algorithm: From a "right to an explanation" to a "right to better decisions"'*, in IEEE Security and Privacy, 2018, 16(3), pp. 46-54; E. PALMERINI, *Algoritmi e decisioni automatizzate. Tutele esistenti e linee evolutive della regolazione*, in *I diritti fondamentali nell'era della digital mass surveillance*, a cura di Ríos Vega, Luis Efren, Scaffardi, Lucia, Spigno, Irene, Napoli, 2021, p. 209 ss.; M. PALMIRANI, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in *XXVI lezioni di Diritto dell'Intelligenza Artificiale*, a cura di U. Ruffolo, Torino, 2021 p. 66 ss.

[27] Cfr. D. MULA, *Elaborazione e sfruttamento dei dati mediante algoritmi*, in *La circolazione dei dati*, cit. p. 127 ss., spec. p. 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…".*

Faccio riferimento a cose recenti ma già note per il grande dibattito che le ha precedute: il *Data Governance Act* è stato definitivamente approvato[28].

C'è infatti da dire che la prospettiva qui proposta consente anche una diversa e a nostro avviso adeguata e corretta interpretazione dell'art. 22 GDPR in quanto anche l'atto di autonomia con il quale si manifesta il "consenso esplicito" dell'art. 22 GDPR – accogliendo la prospettiva qui promossa – dovrà essere sottoposto al sindacato di liceità con la conseguenza che dovrebbe ritenersi invalido l'esplicito consenso del Sig. Leon a farsi perseguitare in quanto persona impulsiva e di basso reddito. Seppure il discorso abbisognerebbe di più ampia trattazione, sembra corretto affermare più generalmente che quando il consenso viene richiesto e prestato per generiche e non meglio specificate finalità di profilazione, di *marketing* o di *targeting*, così come quando si utilizza la base del legittimo interesse ex art. 6 par. 1 lett. *f)*, il consenso si deve ritenere validamente prestato, e la base del legittimo interesse si deve intendere validamente utilizzata, soltanto per (e limitatamente a) specifiche finalità di profilazione, di *marketing* e *targeting* legittime e con esclusione di ogni specifica finalità (di profilazione, di *marketing* e *targeting*) illegittima[29].

In questo contesto, sembra opportuno ricordare il parere congiunto EDPB-GEPD n. 5/2021 del 18 giugno 2021 sulla proposta di *Artificial Intelligence Act*[30].

Questo parere, praticamente coevo alle Linee Guida prima commentate, indica senza dubbio come anche l'EDPB e il Garante europeo siano sensibili alla prospettiva funzionale. È un parere molto importante. Mi limito qui a richiamare la parte in cui si avversano i sistemi di IA di rilevamento delle emozioni (lo stesso si fa per la categorizzazione biometrica) per l'immediata comparazione che può farsi relativamente all'esempio 8 delle citate Linee Guida, ossia l'esempio dell'impulsivo Sig. Leon.

Nel punto 35 di questo parere congiunto così si legge: "[…] *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*".

È evidente come questa chiara – e del tutto condivisibile – presa di posizione mal si concili con una soluzione ermeneutica che consente di sfruttare l'impulsività del Sig. Leon sulla base di un suo consenso esplicito ex art. 22 GDPR. Da qui la promozione di una diversa interpretazione anche dell'art. 22 GDPR, nei termini sopra riassunti.

Sia consentito infine di notare molto brevemente che qui non sono in gioco soltanto i dati personali del Sig. Leon, e nemmeno, più generalmente, i diritti fondamentali del solo Sig. Leon, perché l'invalidità a motivo della illiceità è a tutela di un interesse della collettività: la collettività non vuole che i dati personali di alcuno vengano utilizzati per identificare e avvantaggiarsi di situazioni soggettive di vulnerabilità decisionale e comportamentale delle persone, *anche di persone diverse dall'interessato* dei cui dati personali si tratti.

E di conseguenza aggiungiamo qualcosa che potrà apparire troppo spinta in avanti, ma che, a ben vedere è solo coerente all'impostazione proposta, e si ricava dalle norme esistenti: anche laddove i dati personali venissero immediatamente e definitivamente anonimizzati, deve ritenersi che la collettività non ammette che essi vengano utilizzati *per addestrare sistemi di IA persecutori, manipolativi, discriminatori: perché sono finalità illecite*.

Dobbiamo in definitiva mettere bene a fuoco che l'uso illecito di dati personali - e per uso illecito intendo anche l'*addestramento di sistemi di IA lesivi di diritti fondamentali di persone diverse dall'interessato* - è da vietarsi nel superiore interesse della collettività, *perché non vogliamo che il nuovo volto della nostra società sia costruito da sistemi di IA distorsivi e discriminatori, addestrati con i dati personali* (anonimizzati o meno: non importa) *di nessuno*: nell'epoca dei sistemi di IA (addestrati con dati personali, anonimizzati o meno) non è più in gioco soltanto il *controllo* sui propri dati personali, ma l'*uso* che ne fanno i sistemi di IA.

Un'altra conseguenza sul piano applicativo, ma possiamo fare solo un rapido cenno, è sulla direttiva (UE) 2019/770, dove si parla di impegno del consumatore "di fornire dati personali" (ugualmente nella nostra legge di attuazione: art. 135-*octies* co. 4

[28] Regolamento (UE) 2022/868 del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724.

[29] Si ricorda che secondo l'*Information Commisioner's Office* "*Lawfulness also means that you don't do anything with the personal data which is unlawful in a more general sense*": ICO, *Guide to the General Data Protection Regulation (GDPR)*, disponibile al link https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

[30] https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_it

codice del consumo[31]): non riteniamo corretto leggere - come da alcuni proposto - che si tratta dell'impegno del consumatore "a prestare il consenso": quella norma presuppone che il consenso sia stato già prestato e deve essere un consenso *privacy* come previsto dalla normativa, quindi non solo libero, informato, inequivocabile e specifico, ma anche per finalità legittime: un atto di autonomia assistito da una causa lecita. Il tema della struttura[32], si ripete, non può essere qui affrontato, ma ci sembra significativo aver svolto, con queste osservazioni, quello della funzione.

6. Conclusioni e aperture

Per la comprensione e traduzione del fenomeno della *data economy* in termini di razionalità giuridica, sembra necessario ed utile promuovere, *in aggiunta* alla tradizionale interpretazione dei requisiti dell'atto di autonomia che fa leva sulla *libertà del consenso*, una lettura della normativa esistente orientata anche alle *funzioni*. La *prospettiva funzionale* (che presuppone l'abbandono della più tradizionale concezione autorizzatoria del consenso *privacy* in favore dell'affermazione della sua natura di atto di autonomia) consente di vedere le ragioni tipiche di favore *degli interessati* e *del legislatore* verso determinate finalità di trattamento (*funzioni lecite*), e, al contempo, di disegnare i *limiti dell'area dell'autonomia privata* in termini di reazione giuridica a finalità lesive di diritti fondamentali e di interessi super-individuali, ossia della collettività (*funzioni illecite*).

La prospettiva funzionale sembra ulteriormente necessaria nel quadro dell'erigendo diritto europeo dei dati, nel quale si delinea ormai con nettezza un *divieto di uso dei dati personali con finalità o effetti distorsivi del comportamento delle persone e con finalità o effetti discriminatori*. Accettata come valida e giustificata dalla normativa esistente la prospettiva funzionale, il tema che si propone e che si apre è – naturalmente – quello dell'individuazione e della promozione delle condizioni per assicurare una coerenza e una possibilità di efficiente funzionamento del sindacato di legittimità sulle finalità del trattamento dei dati personali e di liceità dell'atto di autonomia nel quadro delle molte normative che vanno componendo il diritto europeo dei dati, e delle inerenti attribuzioni di competenze tra le diverse autorità (nazionali ed europee) ed organi giurisdizionali.

Due ultime osservazioni sulla parola 'causa' e sull'ingegnerizzazione delle specifiche finalità di trattamento dei dati personali.

A proposito dell'atto di autonomia in che consiste il consenso al trattamento dei dati personali, al posto o come sinonimo della parola 'causa', può usarsi, e abbiamo usato, la parola 'funzione', o 'finalità'; ed è un uso che, anche nella prospettiva della promozione di una interpretazione ed applicazione uniformi del diritto europeo, andrebbe privilegiato. Quando interpretiamo il GDPR, dobbiamo mirare a farci capire in Europa e nel mondo e dobbiamo aspirare a soluzioni ermeneutiche di massima armonizzazione[33]. Parliamo di un controllo e di un giudizio di liceità del consenso *privacy* che abbia come oggetto granulare le specifiche finalità del trattamento.

La granularità dell'oggetto del giudizio di liceità si ricava dalla stessa lettera del GDPR, che, non a caso, parla di "*specifiche*" finalità di trattamento; ed è nelle "cose" di cui parliamo, perché si riscontra nella loro ingegnerizzazione, ossia nell'ingegnerizzazione delle finalità di trattamento. Nel mondo in cui viviamo, caratterizzato dall'ubiquità del *software*, il tema del trattamento dei dati personali assume la più vasta dimensione relativamente ai dati personali digitalizzati. Il loro

[31] L'art. 1 D.Lgs. 173/2021 del 4 novembre 2021 ha introdotto, dopo il capo I del titolo III della parte IV c. cons., il nuovo capo I-bis (art. 135-*octies* ss. c. cons.), relativo ai contratti di fornitura di contenuto digitale e di servizi digitali. L'art. 135-*octies*,co. 4 c. cons. così reca: "*Le disposizioni del presente capo si applicano altresí nel caso in cui il professionista fornisce o si obbliga a fornire un contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si obbliga a fornire dati personali al professionista, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dal professionista ai fini della fornitura del contenuto digitale o del servizio digitale a norma del presente capo o per consentire l'assolvimento degli obblighi di legge cui è soggetto il professionista e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti*".

[32] Per una prima indicazione sulla varietà delle ricostruzioni proposte in dottrina sulla struttura del consenso *privacy* in rapporto alla disciplina recata dalla direttiva (UE) 2019/770 cfr. G. RESTA, *I dati personali oggetto del contratto*, cit., p. 55 ss., spec. p. 75; C. IRTI *Consenso "negoziato" e circolazione dei dati personali*, cit.; V. RICCIUTO, *L'equivoco della privacy. Persona vs dato personale*, cit.; A. DE FRANCESCHI, *Personal data as Counter-Performance*, in *Privacy and Data Protection in Software Services*, cit.

[33] Sappiamo che la parola 'causa' può comportare discussioni interminabili oltre che problemi di traduzione in altre lingue, e in particolare nella lingua inglese; ma questo non vuol dir nulla perché è riconosciuto da tutti e a qualunque latitudine un sindacato sulla funzione degli atti di autonomia; anche i francesi, che hanno eliminato formalmente il requisito della causa dal *code civil* (per rendere il loro ordinamento più attraente), non hanno affatto con ciò eliminato, bensì hanno confermato, il sindacato di liceità sulla funzione o fine (*but*) del contratto. Cfr., da ultimo e per tutti, R. FORNASARI, *Causa, meritevolezza e razionalità del contratto*, Milano, 2022, p. 267 ss.

trattamento viene affidato ad algoritmi, progettati per perseguire specifiche finalità (specifiche finalità di trattamento dei dati personali).

Tale ingegnerizzazione - al contrario di quanto potrebbe dirsi a prima vista - consente un maggiore controllo ed un più efficace, effettivo e granulare contrasto delle finalità di trattamento *illegittime*. Ciò in quanto le specifiche finalità di trattamento vengono ingegnerizzate in *prodotti* software. Il tema che si apre a partire da queste osservazioni, è quello del contrasto di determinati prodotti *software*, ed in particolare del contrasto di determinati sistemi *software* di intelligenza artificiale (*machine learning*) che perseguono finalità di trattamento illegittime, come i sistemi di intelligenza artificiale che sono idonei a distorcere il comportamento delle persone e i sistemi di intelligenza artificiale discriminatori. Come noto, tale tema è stato da ultimo affrontato nella proposta di *Artificial Intelligence Act*[34], relativamente ai sistemi *software* di intelligenza artificiale, nella prospettiva della legislazione europea dei prodotti, sotto l'angolo regolatorio delle condizioni per l'immissione sul mercato, la messa in servizio e l'uso di determinati sistemi di intelligenza artificiale sulla base di un approccio c.d. *risk based*, avuto cioè riguardo a certi fattori di rischio, intesi quali fattori di pericolosità dei prodotti, specificamente per la loro idoneità a ledere diritti fondamentali delle persone[35]. Indipendentemente dal giudizio che possa darsi sull'architettura e sulle specifiche soluzioni di cui alla proposta normativa in questione[36], ci sembra che si tratti, relativamente al nostro tema, di una indicazione che conferma la necessità di promuovere un controllo e un giudizio granulare sul consenso *privacy* nella direzione funzionale indicata in questa sede: ossia affermando che il consenso *privacy* ai sensi degli artt. 6, 9 e 22 GDPR debba ritenersi validamente reso solo per specifiche finalità di trattamento di dati personali *legittime*. Con la conseguenza che per legge certe specifiche finalità di trattamento (quali quelle ingegnerizzate nell'algoritmo dell'esempio istituzionale del Sig. Leon, volto a bersagliare specificamente persone impulsive e di basso reddito) devono ritenersi illegittime *e l'atto di consenso dell'interessato deve ritenersi validamente prestato per legge solo e limitatamente a finalità di trattamento legittime*.

È, come può facilmente intendersi, una conclusione che attende uno svolgimento teorico: la teorizzazione di una possibile *nullità parziale* dell'atto di consenso *privacy* relativamente alle sole specifiche finalità illegittime, e una messa a punto delle categorie per predicare l'illiceità e l'invalidità totale o parziale dell'atto di autonomia-consenso *privacy* a partire dal contrasto delle specifiche finalità di trattamento con norme imperative, con principî raccolti in formule quali i "nostri" ordine pubblico e buon costume, e, più generalmente, a partire dalla lesione dei diritti fondamentali riconosciuti dal diritto europeo. In proposito, sembra corretto ammonire di evitare automatismi dogmatici nazionali, perché l'ambito normativo interessato dalla teorizzazione in questione è – lo si sottolinea di nuovo – di diritto europeo.

Ed è, infine, una conclusione che attende anche uno svolgimento tecnologico. Ed infatti, se, come risaputo, all'ingegnerizzazione del trattamento dei dati personali digitali si è già risposto con *software* a tutela della *privacy*, ossia disegnati per individuare trattamenti lesivi del complesso dei diritti tradizionalmente associati alla protezione assicurata agli interessati dal GDPR[37], la medesima tecnologia è senz'altro idonea ad essere impiegata per sottoporre le specifiche finalità di trattamento dei dati personali ingegnerizzate in prodotti *software*, a più ampi test e controlli di legittimità, eccedenti la tutela *privacy*, e comprensivi della tutela di tutti i diritti fondamentali.

Ci sembra che si tratti di svolgimenti tutti necessari alla luce del complesso delle normative europee che si vanno sistemando intorno al GDPR, e anche storicamente giustificati: il consenso *privacy* non può più correttamente intendersi come

[34] Si fa riferimento alla Proposta COM(2021) 206 *final* del 21.4.2021 di Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione sull'intelligenza artificiale (proposta di *Artificial Intelligence Act*).

[35] Cfr. art. 65 par. 1 proposta di *Artificial Intelligence Act*: *"Un sistema di IA che presenta un rischio è inteso come un prodotto che presenta un rischio definito all'articolo 3, punto 19, del regolamento (UE) 2019/1020 per quanto riguarda i rischi per la salute o la sicurezza o per la tutela dei diritti fondamentali delle persone".*

[36] Per una prima indicazione, anche bibliografica, sia consentito rinviare a S. ORLANDO, *Regole di immissione sul mercato e «pratiche di intelligenza artificiale» vietate nella proposta di Artificial Intelligence Act*, in *Persona e mercato* 3/2022, p. 346 ss.

[37] Cfr. da ultimo, anche per maggiori riferimenti bibliografici, A. BERNES, *Privacy Enhancing Technologies, trasparenza e tutela della persona nell'ambiente digitale*, in *Annuario OGID 2022- Yearbook JODI 2022*, a cura di S. Orlando e G. Capaldo, Roma, Sapienza Università Editrice, 2022, p. 23 ss.; e v. anche M. RATTI, *Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita*, in *Codice della Privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino, Milano, 2021, p. 410 ss.; H. HAAPIO, M. HAGAN, M. PALMIRANI, A. ROSSI, *Legal Design Patterns for Privacy*, in E. Schweighofer et Al. (a cura di), *Data Protection / LegalTech, Proceedings of the 21th International Legal Informatics Symposium 2018*, Berna, 2018, pp. 445–450.

una *conventio nuda*, tanto meno nell'epoca dell'economia dei dati.