SULLA NECESSITÀ DI UN CONTROLLO DI LICEITÀ *SOSTANZIALE* PER TUTTE LE BASI DEL TRATTAMENTO DEI DATI PERSONALI

Di Salvatore Orlando

SOMMARIO*: 1. Il trattamento di dati personali per lo sviluppo e l'uso di sistemi di IA: la questione della base del trattamento ai sensi del GDPR. – 2. La questione della liceità del trattamento di dati personali per lo sviluppo e l'uso di sistemi di IA sottoposti ai divieti di immissione sul mercato, messa in servizio e uso di cui all'AI Act. – 3. I divieti (diretti ed indiretti) di trattamento dei dati personali alla stregua del diritto unitario e nazionale. – 4. L'inidoneità delle condizioni di cui agli artt. 6(1) e 9(2) GDPR a costituire in concreto valide basi per il trattamento lecito di dati personali a fronte di norme imperative che vietano direttamente o indirettamente determinati trattamenti. – 5. Giustificazione funzionale e conformità ordinamentale di ciascuna delle basi del trattamento – 6. La liceità sostanziale del trattamento e sua distinzione dalla liceità formale – 6.1. Primo esempio: sistema di IA di marketing online che impiega algoritmi idonei a distorcere il comportamento delle persone fisiche causando loro un danno significativo – 6.2. Secondo esempio: sistema di IA di marketing online che impiega algoritmi idonei a distorcere il comportamento delle persone fisiche senza causare loro un danno significativo – 6.3. Terzo esempio: sistema di IA di marketing politico online che impiega algoritmi che profilano le persone fisiche sulla base delle speciali categorie di dati personali dell'art. 9(1) GDPR – 7. Adeguatezza del giudizio di liceità sostanziale al suo oggetto: il carattere analitico del test di liceità sostanziale in concreto con riferimento ai singoli trattamenti e ai singoli algoritmi – 8. La distribuzione delle competenze e il coordinamento delle attività tra autorità amministrative e giurisdizionali. – 9. (segue) L'esempio del Sig. Leon. – 10. (segue) Il chi e il cosa: la distinzione tra controllo di conformità ordinamentale e giudizio di liceità ai sensi del GDPR (o dell'EUDPR). – 11. Conclusioni.**

ABSTRACT. *In questo saggio, l'a., utilizzando esempi relativi al trattamento dei dati personali per lo sviluppo e l'uso di sistemi di intelligenza artificiale, espone il concetto di liceità sostanziale del trattamento dei dati personali, intesa nel senso del rispetto o non violazione delle norme dell'ordinamento che pongono direttamente o indirettamente divieti al trattamento dei dati personali, distinguendo questo concetto da quello della liceità in senso formale del trattamento dei dati personali, consistente nella ricorrenza di una base astrattamente idonea al trattamento ai sensi del GDPR. L'a. osserva che nessuna delle basi per il trattamento previste dal GDPR è compatibile con la violazione di norme imperative, poiché ciascuna di essa esprime il carattere della giustificazione funzionale e quello della conformità ordinamentale, e aggiunge che il giudizio di liceità sostanziale del trattamento di dati personali deve svolgersi in concreto e presuppone che sia stato previamente assolto con esito positivo quello di liceità formale. Dopo aver evidenziato le principali questioni applicative conseguenti al test di liceità sostanziale (inclusa la questione della distribuzione di competenze tra le autorità di controllo per la protezione dei dati personali, le altre autorità indipendenti che presidiano altri settori dell'ordinamento e l'autorità giurisdizionale, in relazione al test dell'osservanza o non violazione delle norme*

ISSN 2239-8570

imperative di diritto unitario e nazionale di volta in volta rilevanti), e aver fatto numerosi esempi, l'a. sottolinea che la teoria della liceità sostanziale consente di togliere pressione alla base del consenso, spesso ritenuta, a torto, come l'unica base veramente idonea a realizzare la protezione dei dati personali, perché, da un lato, l'illiceità sostanziale può colpire tutte le basi invocate dai titolari per il trattamento, e, dall'altro, perché il giudizio di liceità sostanziale sulla base del consenso, se svolto correttamente, consente di censurare puntualmente come contra legem una pluralità di trattamenti che perseguono in concreto finalità illegittime o sono altrimenti vietati dalla legge, in questo modo permettendo di superare tecnicamente anche la communis opinio che vede nel consenso non soltanto l'unica arma della privacy, ma, per colmo, anche un'arma spuntata.

In this essay, the author, illustrates the concept of substantive lawfulness of personal data processing by making examples relevant to the processing of personal data for the development and use of artificial intelligence systems. In the author's view, substantive lawfulness means observance and non-violation of the many provisions of Union and national law that directly or indirectly provide prohibitions on the processing of personal data, and must be distinguished from formal lawfulness, meaning the occurrence of one of the bases for assessing an 'in principle' lawful processing of personal data pursuant to the GDPR. The a. observes that each processing of personal data shall pass a test of substantive lawfulness since each and all of the bases provided for by the GDPR bear the characters of functional justification and conformity to the law system. The a. argues that the test of substantive lawfulness shall be made in concrete and it presupposes that a test of formal lawfulness has been already carried out. After having examined the main practical implications relevant to the carrying out of the test of substantive lawfulness (including the issue of the distribution of powers among the supervisory authorities for data protection, on one side, and the other supervisory authorities as well as the judiciary, in connection with the assessment of the violation of mandatory provisions in the many sectors of the law-system from time to time applicable and relevant for the test of substantive lawfulness), and after having made many examples, the a. underlines that the theory of the substantive lawfulness may take the pressure off the legal basis of consent, which is often, and wrongly, considered to be the only legal basis designed for truly protecting personal data. In fact, on one side, substantive unlawfulness may affect each and all of the legal bases invoked by the data processor for processing personal data; on the other side, the test of substantive lawfulness, where correctly carried out through an analytical check of compliance with all applicable mandatory provisions, is capable to result, in practice, in the finding of a number of unlawful processing activities, i.e. processing activities that either pursue unlawful purposes or are otherwise prohibited by the law, thus also overcoming the common opinion according to which consent not only is the only tool designed for being a privacy shield but also is a useless one.

ISSN 2239-8570

1. Il trattamento di dati personali per lo sviluppo e l'uso di sistemi di IA: la questione della base del trattamento ai sensi del GDPR.

Nel presente scritto vorrei esporre il concetto di liceità 'sostanziale' del trattamento dei dati personali.

Per la dimostrazione, mi avvarrò, per cominciare, di esempi relativi al trattamento dei dati personali per lo sviluppo e l'uso di sistemi di intelligenza artificiale. Come verrà spiegato meglio nel prosieguo (v. in particolare *infra* dal par. 5 in avanti), la dimostrazione ha tuttavia carattere generale.

Secondo la terminologia dell'AI Act[1] (di seguito anche **AIA**), lo sviluppo e l'uso dei sistemi di intelligenza artificiale (o **sistemi di IA**)[2] include o richiede il trattamento di dati personali per finalità di addestramento, convalida, prova e input[3].

Il primo possibile livello di illiceità del trattamento di dati personali per lo sviluppo e l'uso di sistemi di IA riguarda la scelta di una condizione, tra quelle previste dal GDPR[4] (di seguito anche il **Regolamento**), idonea a costituire una base per il lecito trattamento.

Ed infatti, come noto, al principio di liceità del trattamento dei dati personali, enunciato all'art. 5(1)(a) del Regolamento[5], 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 una delle condizioni previste nelle lettere da a) a f) del medesimo paragrafo: le cosiddette 'basi' del trattamento.

---

[1] Regolamento (UE) 2024/1689 del 13 giugno 2024 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).

[2] Secondo la definizione di cui al numero 1) dell'art. 3 AIA, un «sistema di IA» è "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali".

[3] Vedi le relative definizioni ai numeri 29), 30), 32) e 33) dell'art. 3 AIA: "29) «dati di addestramento»: i dati utilizzati per addestrare un sistema di IA adattandone i parametri che può apprendere"; "30) «dati di convalida»: i dati utilizzati per fornire una valutazione del sistema di IA addestrato e per metterne a punto, tra l'altro, i parametri che non può apprendere e il processo di apprendimento, al fine tra l'altro di evitare lo scarso (underfitting) o l'eccessivo (overfitting) adattamento ai dati di addestramento"; "32) «dati di prova»: i dati utilizzati per fornire una valutazione indipendente del sistema di IA al fine di confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio";"33) «dati di input»: i dati forniti a un sistema di IA o direttamente acquisiti dallo stesso, in base ai quali il sistema produce un output".

[4] Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[5] 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

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

Questo modo tradizionale di analizzare la conformità al GDPR dello sviluppo e dell'uso dei sistemi di IA individua un primo livello di possibile illiceità del trattamento. Un esempio di analisi di questo tipo può vedersi con le prime contestazioni mosse dalle autorità di controllo per la protezione dei dati personali ad OpenAI LLC ai sensi del GDPR in relazione al servizio ChatGPT[6], e ai dubbi suscitati dalla spiegazione fornita dalla medesima società di ricorrere alla base del legittimo interesse per il trattamento di dati personali[7], da cui il recente rapporto della *task force* costituita *ad hoc* in seno all'EDPB per valutare la questione[8].

In particolare, nel suo report del 23 maggio 2024, la task force dell'EDPB ha evidenziato una serie di criticità del servizio ChatGPT circa il rispetto delle prescrizioni del GDPR, toccando, unitamente ai temi della correttezza, della trasparenza, degli obblighi di informazione, dell'accuratezza e dei diritti degli interessati, quello della liceità del trattamento. Sotto questo aspetto, il rapporto ha sottolineato la necessità che ricorra una delle basi previste dal primo paragrafo dell'art. 6 del Regolamento, 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[9].

Similmente, il Garante europeo per la protezione dei dati personali (**EDPS**), nel suo documento del 3 giugno 2024 nel quale si è proposto di offrire dei primi orientamenti alle istituzioni, gli organi e gli organismi UE per garantire il rispetto del regolamento (UE) 2018/1725 (**EUDPR**) relativamente all'uso di sistemi di IA c.d. generativa[10], dopo aver strutturato il documento attraverso la posizione e la risposta a 13 domande, ha

---

[6] 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).

[7] Cfr. anche F. G'SELL, *Regulating under Uncertainty: Governance Options for Generative AI*, Stanford, Cyber Policy Center, luglio 2024 (https://cyber.fsi.stanford.edu/content/regulating-under-uncertainty-governance-options-generative-ai), p. 180, note n. 1019 e 1020.

[8] https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf.

[9] 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».

[10] Sono i *First EDPS Orientations for ensuring data protection compliance when using Generative AI systems* del 3.6.2024: https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf.

ISSN 2239-8570

impostato la n. 6 («quando è lecito il trattamento dei dati personali nelle fasi di progettazione, sviluppo e validazione di sistemi di IA generativa ?») nella prospettiva dell'individuazione di una base adeguata, tra quelle dell'art. 5 EUDPR (corrispondente all'art. 6 GDPR).

Al di là delle specificità del servizio ChatGPT e della c.d. IA generativa, e indipendentemente dall'esame nel merito dei singoli argomenti esposti in questi documenti, non c'è dubbio che, generalmente, un primo livello del giudizio circa la liceità/illiceità del trattamento di dati personali per l'uso di sistemi di IA sia da individuarsi nelle condizioni a ciò idonee ai sensi dell'art. 6 GDPR (art. 5 EUDPR) e delle altre disposizioni del GDPR che assolvono a questa funzione (art. 9 GDPR *in primis*).

Nel prosieguo del presente articolo, piuttosto che approfondire ulteriormente le questioni relative a questo tipo di indagine, esporrò quelli che ritengo essere due ulteriori livelli dell'analisi circa la liceità/illiceità del trattamento di dati personali per lo sviluppo e l'uso di sistemi di IA e indicherò alcune questioni interpretative collegate.

2. La questione della liceità del trattamento di dati personali per lo sviluppo e l'uso di sistemi di IA sottoposti ai divieti di immissione sul mercato, messa in servizio e uso di cui all'AI Act.

L'art. 5 dell'AI Act vieta l'immissione sul mercato, la messa in servizio e/o[11] l'uso di una serie di sistemi di intelligenza artificiale.

Si tratta, in particolare di:

- sistemi di IA che utilizzano «tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo»[12];
- sistemi di IA «che sfrutta[no] le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo»[13];

[11] Nelle previsioni di cui alle lettere da (a) ad (h) del primo paragrafo dell'art. 5 AIA (riportate di seguito nel testo), l'uso è sempre vietato, mentre l'immissione sul mercato e la messa in servizio sono sempre vietate tranne che nel caso della lettera (h) ossia nella previsione dei «sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto», con le eccezioni ivi specificate.

[12] Art. 5(1)(a) AIA.

[13] Art. 5(1)(b) AIA.

ISSN 2239-8570

- «sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti:

i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti;

ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità»[14];

- sistemi di IA «per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa»[15];
- «sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante scraping non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso»[16];
- «sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza»[17];
- «sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale; tale divieto non riguarda l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto»[18];
- «sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti:

[14] Art. 5(1)(c) AIA.
[15] Art. 5(1)(d) AIA.
[16] Art. 5(1)(e) AIA.
[17] Art. 5(1)(f) AIA.
[18] Art. 5(1)(g) AIA.

ISSN 2239-8570

i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse;

ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico;

iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni»[19].

Le espressioni e i concetti rilevanti per questo livello di analisi, come utilizzati e ricavabili dall'AI Act, sono: «immissione sul mercato»[20], «messa in servizio»[21], «uso», «sviluppo», «fornitore»[22] e «deployer»[23], in ciascun caso sottintendendo «di sistemi di IA», nonché: «dati di addestramento», «dati di convalida», «dati di prova», «dati di input»[24].

Immissione sul mercato, *messa in servizio* e *uso* sono le tre attività vietate dall'art. 5 AIA. Le prime due espressioni sono definite dal Regolamento, la terza no.

La parola *uso* è particolarmente rilevante anche nel contesto del primo Considerando dell'AI Act, dove si trova espresso al riguardo un divieto agli Stati membri. Lo stesso è a dirsi per la parola *sviluppo*, nemmeno essa definita.

Si trova scritto alla fine del primo Considerando dell'AI Act che agli Stati membri è proibito prevedere o mantenere ulteriori restrizioni allo «sviluppo», alla «commercializzazione» e all'«uso» dei sistemi di IA rispetto a quelle previste dal medesimo regolamento[25].

Mentre le espressioni *sviluppo* e *uso*, come notato, non sono definite - e su di esse merita fare qualche osservazione ulteriore – non ci sono difficoltà a ritenere che *commercializzazione* stia a significare qualsiasi attività

[19] Art. 5(1)(h) AIA.

[20] Art. 3, n. 9) AIA: "«immissione sul mercato»: la prima messa a disposizione di un sistema di IA o di un modello di IA per finalità generali sul mercato dell'Unione".

[21] Art. 3, n. 11) AIA: "«messa in servizio»: la fornitura di un sistema di IA direttamente al deployer per il primo uso o per uso proprio nell'Unione per la finalità prevista".

[22] Art. 3 n. 3) AIA: "«fornitore»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito".

[23] Art. 3 n. 4) AIA: "«deployer»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale".

[24] Come definiti ai numeri 29), 30), 32) e 33) dell'art. 3 AIA, sopra richiamati alla nota 3.

[25] Considerando 1 AIA "[…] Il presente regolamento garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento".

ISSN 2239-8570

compresa nei campi di significato delle espressioni, dotate di definizione, *immissione sul mercato* e *messa in servizio* e anche in quella di «messa a disposizione sul mercato», anch'essa definita[26], e comprendente genericamente l'attività di distribuzione.

Il significato di uso sembra potersi ricavare indirettamente dall'esame di due disposizioni:

- quella che delinea la (sopra richiamata) definizione di deployer come soggetto che utilizza un sistema di IA per fini professionali; e
- quella che include nel campo di applicazione soggettivo dell'AIA i fornitori e i deployer stabiliti o situati fuori dall'Unione laddove «l'*output* prodotto dal sistema di IA sia *utilizzato* nell'Unione»[27].

In particolare, la prima disposizione sembra rilevante per dire cosa l'uso dei sistemi di IA *è*, e la seconda per dire cosa l'uso dei sistemi di IA *non è*, ossia per distinguerla dall'*utilizzo degli output* dei sistemi di IA.

Da cui anche la conseguenza che l'utilizzo di output di sistemi di IA per fini professionali non equivale all'uso di sistemi di IA, e può perciò essere assoggettato a obblighi e divieti da parte degli Stati membri indipendentemente dalle disposizioni dell'AI Act, non ricadendo nel divieto di cui al primo Considerando, sopra richiamato, e più generalmente non ricadendo nel campo di applicazione dell'AI Act.

Nemmeno il termine *sviluppo*, come si diceva, è definito nell'AI Act. Esso è tuttavia impiegato in più punti dell'AI Act ed in particolare a proposito della definizione, già richiamata, di *fornitore*, da cui si ricava chiaramente la strumentalità dello *sviluppo* (come inteso nell'AI Act) rispetto all'*immissione sul mercato* e alla *messa in servizio* dei sistemi di IA, e, di conseguenza, anche al loro *uso*.

Dalle definizioni disponibili sembra corretto dire che l'uso di sistemi di IA presuppone, dal punto di vista tecnologico, un loro previo sviluppo, nonché, dal punto di vista commerciale, una loro previa immissione sul mercato e messa in servizio.

Sembra anche corretto dire che lo sviluppo di sistemi di IA presuppone attività di addestramento, convalida, prova e input di dati, e che i dati possono essere anche dati personali.

Non è chiaro se nella terminologia dell'AIA l'attività di input, riferita ai dati di input, comprenda il c.d. prompting. Ad ogni modo, sembra corretto dire che l'uso di sistemi di IA implica attività di input e prompting.

Infine, sembra corretto dire che gli output sono tipicamente generati sia nella fase di sviluppo che in quella di uso di sistemi di IA.

Relativamente ai dati personali impiegati per lo sviluppo e l'uso di sistemi di IA e generati da sistemi di IA come output, si possono fare le seguenti osservazioni.

---

[26] Art. 3 n. 10) AIA: "«messa a disposizione sul mercato»: la fornitura di un sistema di IA o di un modello di IA per finalità generali per la distribuzione o l'uso sul mercato dell'Unione nel corso di un'attività commerciale, a titolo oneroso o gratuito".

[27] Art. 2(1)(c) AIA : «Il presente regolamento si applica: […] c) ai fornitori e ai deployer di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione».

ISSN 2239-8570

Poiché l'immissione sul mercato, la messa in servizio e l'uso di sistemi di IA (attività espressamente vietate relativamente ai sistemi di IA e nei casi previsti dall'art. 5 AIA) sono attività che presuppongono e richiedono necessariamente un'altra attività, ossia lo sviluppo dei medesimi sistemi di IA, e lo sviluppo è attuato attraverso il trattamento di dati personali per fini di addestramento, convalida, prova e input, sembra corretto ritenere che i relativi divieti dell'art. 5 AIA siano al contempo idonei a far ritenere *contra legem* e dunque illecito il trattamento di dati personali finalizzati alle attività vietate (immissione sul mercato, messa in servizio e uso) relativamente ai sistemi di IA assoggettati ai medesimo divieti.

Ossia, in breve, che debba ritenersi generalmente vietato il trattamento di dati personali realizzato per lo sviluppo e l'uso dei sistemi di IA assoggettati ai divieti dell'art. 5 AIA. E concludersi che un simile trattamento sia da ritenersi illecito *anche ai sensi del GDPR*.

La conclusione di cui sopra - per ragionevole che possa apparire - nasconde una serie di questioni interpretative abbastanza complesse, che anticiperemo nei loro tratti essenziali in questo paragrafo e svilupperemo nei paragrafi da 4 a 10 *infra*.

La prima consiste nello stabilire se il requisito di liceità del trattamento - ricavato dal principio espresso nell'art. 5(1)(a) GDPR[28] - possa interpretarsi nel senso di riferirlo non soltanto alla necessaria presenza di una delle condizioni (o 'basi') per il trattamento di cui all'art. 6(1) GDPR, ma anche nel senso generale di rispetto di norme imperative, e, in questo caso, chiedendosi ulteriormente se si debba avere in considerazione il solo diritto unitario o anche il diritto nazionale applicabile.

Si tratta di una questione particolarmente significativa dal punto di vista sistematico, per le importanti implicazioni che la risposta affermativa comporta sia nel senso di rendere necessario un giudizio esteso ad altre fonti diverse dal GDPR e potenzialmente all'intero ordinamento (e dunque un giudizio non limitato al Regolamento, sebbene da esso autorizzato), sia nel senso di postulare la rilevanza di interessi in ipotesi ulteriori rispetto a quelli dell'interessato[29] (i.e. la persona fisica dei cui dati personali si tratta[30]), in quanto tutelati dalle norme imperative la cui violazione comporta in ipotesi l'illiceità del trattamento[31].

---

[28] 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»);[…]".

[29] Su cui v. per tutti, già prima del GDPR, C.M. BIANCA, *Nota introduttiva I*, p. XIX ss., spec. XXII ss., in *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196 («Codice* privacy*»)*, a cura di C.M. Bianca e F.D. Busnelli, t. I, Cedam, Padova, 2007; P.M. VECCHI, *sub art. 2*, in *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196*, cit., p. 4 ss.

[30] Art. 4, n. 1) GDPR "«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)".

[31] In epoca pre-GDPR, v. P. 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, 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 l'a. 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

In proposito, e nel senso di una risposta affermativa, mi sembra corretto osservare che le medesime implicazioni devono ritenersi in ogni caso doverose:

- da un lato, in considerazione del principio di cui alla successiva lettera (b) dell'articolo 5(1) GDPR, nella parte in cui il Regolamento prescrive che i dati personali debbano essere «raccolti per finalità […] *legittime*, e successivamente trattati in modo che non sia incompatibile con tali finalità»[32]; e,

- dall'altro lato, anche se si guarda soltanto alle singole basi del trattamento, di cui all'art. 6(1) GDPR.

Ed in effetti, sotto il primo aspetto, non sembrano esserci ragioni per limitare il giudizio di legittimità delle finalità del trattamento - prescritto dall'art. 5(1)(b) GDPR - ad un test endo-regolamentare, mentre, sotto il secondo aspetto, non si vede come potrebbero integrare una valida base per un trattamento lecito *ex* art. 6(1)(a) GDPR un consenso prestato dall'interessato per una o più specifiche finalità *illegittime*, o, *ex* art. 6(1)(b) GDPR, l'esecuzione di un contratto *illecito*, o ancora, *ex* art. 6(1)(f) GDPR, l'invocazione di un interesse legittimo a proposito di un trattamento necessariamente e tipicamente implicato da attività *contra legem*[33].

Similmente deve dirsi per la base del trattamento *ex* art. 6(1)(e) GDPR, consistente nell'esecuzione di un compito di interesse pubblico o connesso

luogo), sia in grado di prescindere dalle preferenze di quest'ultimo, in ipotesi in cui queste contrastino con l'interesse della collettività».

[32] 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»); […]". 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".

[33] Significativa in proposito appare la recente sentenza della Corte di giustizia dell'Unione europea (**CGUE**), Nona sezione, del 4 ottobre 2024 nella causa C-621/22, in particolare quanto al ragionamento riassunto nelle ultime parole della dichiarazione finale di seguito riportata: "L'articolo 6, paragrafo 1, primo comma, lettera f), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva95/46/CE (regolamento generale sulla protezione dei dati), deve essere interpretato nel senso che: un trattamento di dati personali consistente nella comunicazione a titolo oneroso di dati personali dei membri di una federazione sportiva, al fine di soddisfare un interesse commerciale del titolare del trattamento, può essere considerato necessario ai fini del legittimo interesse perseguito da tale titolare, ai sensi di detta disposizione, solo a condizione che tale trattamento sia strettamente necessario alla realizzazione del legittimo interesse in questione e che, alla luce di tutte le circostanze pertinenti, non prevalgano su tale legittimo interesse gli interessi o le libertà e i diritti fondamentali dei suddetti membri. *Sebbene detta disposizione non esiga che un interesse siffatto sia determinato dalla legge, essa richiede che il legittimo interesse invocato sia lecito*".

ISSN 2239-8570

all'esercizio di pubblici poteri, in considerazione di quanto disposto dai successivi paragrafi 2 e 3 dell'art. 6 del Regolamento (a proposito sia di questa base che di quella dell'interesse legittimo) in particolare con riferimento al ruolo attribuito al diritto unitario e nazionale di specificare tali basi e le condizioni alle quali il relativo trattamento possa ritenersi lecito[34].

Ciò sta a significare che, anche con riferimento alla base del trattamento ex art. 6(1)(e) GDPR, deve ritenersi non invocabile validamente la base dell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, relativamente a trattamenti necessariamente e tipicamente implicati da attività *contra legem*. Si possono fare gli esempi di certi casi d'uso di sistemi di IA inerenti alla c.d. attività di contrasto (in inglese *public enforcement*) espressamente vietati dalla legge, quale quelli previsti espressamente dall'art. 5(1) AIA alle lettere (d) e (h), sopra richiamati, ossia, rispettivamente, per la predizione di reati e per l'identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto.

Quanto sopra, in sintesi, e fatti salvi i necessari approfondimenti (v. *infra* parr. 4-10), fa ritenere che i divieti posti dall'art. 5 dell'AI Act siano rilevanti per stabilire l'illiceità di certi trattamenti di dati personali *ai sensi del GDPR*.

Si pongono, di conseguenza, ulteriori questioni interpretative per stabilire con maggiore precisione quali trattamenti debbano ritenersi illeciti.

Si tratta di questioni complesse, anche a cagione di una certa oscurità del linguaggio utilizzato dal legislatore europeo nell'AI Act[35] e della stessa materia che ne forma oggetto: sicuramente di non facile comprensione – nemmeno limitatamente ai profili giuridicamente rilevanti - per coloro che non hanno una preparazione specifica nella scienza informatica e nel settore particolare della scienza informatica chiamato intelligenza artificiale.

---

[34] Art. 6(2) GDPR: «Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento *lecito* e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX». Art. 6(3)(3) GDPR: «La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita: a) dal diritto dell'Unione; o b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla *liceità* del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito».

[35] Si consideri che molte delle definizioni e degli stessi termini utilizzati nell'AIA sono stati modificati più volte rispetto a quelli che si leggevano nel testo della proposta della Commissione dell'aprile del 2021.

ISSN 2239-8570

Solo per indicare alcune tematiche: va risolto il tema del confine tra ricerca (non assoggettata ad alcun divieto[36]) e sviluppo (nozione precipua intesa nell'AIA come distinta dalla ricerca in quanto funzionalmente preordinata alla immissione sul mercato, messa in servizio e, dunque, all'uso, di sistemi di IA); il tema dei confini e delle responsabilità relative alle attività di prova (intesa dall'AIA come tipicamente affidata a soggetti terzi rispetto al fornitore); il tema specifico del prompting (e le sue differenze, se rilevanti ai fini del trattamento dei dati personali, con l'input); il tema specifico dei dati di prova (relativamente a trattamenti fatti da terzi indipendenti, incaricati delle attività di prova dei sistemi di IA); il tema specifico dei dati di output (ci si può chiedere se il divieto di trattamento relativamente ai sistemi di IA e ai casi previsti dall'art. 5 AIA, voglia dire anche divieto di generare ossia produrre dati personali) etc.

Nel presente contributo non potrò entrare nel dettaglio delle disposizioni dell'AI Act che ineriscono a questo secondo livello di analisi, essendomi prefissato l'obiettivo di segnalare *l'esistenza stessa di questo specifica dimensione di illiceità, ai sensi del GDPR, del trattamento dei dati personali per l'uso e lo sviluppo di sistemi di IA*, a fronte di un dibattito che generalmente si sofferma solo sull'individuazione della base del trattamento (primo livello: par. 1, *supra*).

Motivo per il quale, tornerò invece più avanti nel presente scritto sulle più rilevanti questioni interpretative che questo livello di analisi ed il successivo, esposto al par. 3 *infra*, comportano sul fronte dell'interpretazione del GDPR (v. *infra* parr. 4-10).

3. I divieti (diretti ed indiretti) di trattamento dei dati personali alla stregua del diritto unitario e nazionale.

Se si riconosce in linea di principio che l'esistenza di divieti di certe attività implicanti necessariamente determinati trattamenti possa far ritenere il trattamento in sé considerato illecito ai sensi del GDPR, non si avrà difficoltà ad applicare il ragionamento svolto nel paragrafo precedente (a proposito dell'illiceità del trattamento di dati personali per lo sviluppo e uso di sistemi di intelligenza artificiale sottoposti ai divieti di cui all'art. 5 AIA) *anche al di fuori dalle disposizioni dell'AI Act*, a tutti i casi di divieti di determinati trattamenti o di determinate attività che comportano necessariamente determinati trattamenti, *tutte le volte in cui i trattamenti in questione siano posti in essere per lo sviluppo e l'uso di sistemi di intelligenza artificiale*.

Facciamo qualche esempio cominciando da normative che vietano direttamente determinati trattamenti.

Come primo esempio, possiamo pensare alla recente legge 193/2023 sul c.d. oblio oncologico[37], relativamente ai divieti di trattare determinate informazioni personali su pregresse malattie oncologiche per la

[36] Artt. 1, 2(6) AIA.

[37] 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*.

ISSN 2239-8570

determinazione di condizioni contrattuali, per la valutazione dei requisiti psicofisici delle persone che vogliono adottare (in procedure di adozione), o per le valutazioni di candidati in procedure concorsuali o selettive, pubbliche o private[38].

Laddove vengano sviluppati, per essere commercializzati e usati, sistemi di IA preordinati a valutazioni di questi tipi di dati personali per queste finalità, non avrei dubbi nel ritenere illecito *anche ai sensi del GDPR* il trattamento dei dati personali, realizzato per lo sviluppo ed uso di simili sistemi di IA[39].

Come secondo esempio, possiamo citare i divieti dell'art. 7 della recente direttiva sui lavoratori delle piattaforme online[40]. Ai sensi di questo articolo, è fatto divieto 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 associazione, 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.

[38] 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. 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.

[39] L'art. 5(4) della legge 193/2023 attribuisce al Garante privacy la competenza per «vigilare» sull'applicazione della medesima legge. Sul punto v. *infra* al par. 8.

[40] https://www.europarl.europa.eu/news/it/press-room/20240419IPR20584/riders-il-parlamento-adotta-la-direttiva-sul-lavoro-delle-piattaforme

ISSN 2239-8570

Anche in questo caso siamo in presenza di una disciplina che prevede specifici divieti di trattamento di dati personali talché, non avrei dubbi nel definire *illeciti anche ai sensi del GDPR* tali trattamenti.

Come terzo, quarto e quinto esempio possiamo pensare ai divieti di trattamento delle speciali categorie di dati personali ex art. 9(1) GDPR, posti dal Digital Services Act[41] (**DSA**)[42] e dal recente regolamento sul marketing politico[43], e al divieto di trattare i dati personali dei minori, posto dal DSA[44].

Anche in questi casi dovremo dire che siamo in presenza di norme che prevedono specifici divieti di trattamento di determinate categorie di dati personali per determinate finalità; e anche in questi casi non avrei dubbi a ritenere illecito *ai sensi del GDPR* tali trattamenti di dati personali, compreso, in principio, il caso in cui i relativi trattamenti siano realizzati per lo sviluppo e l'uso di sistemi di IA.

Possiamo notare, ora, che in tutti gli esempi di cui sopra ho citato norme imperative, di diritto dell'Unione o italiano, che vietano *direttamente* determinati trattamenti.

Lo stesso ragionamento deve a mio avviso farsi - e la stessa conclusione in punto di illiceità del trattamento *ai sensi del GDPR* trarsi - anche relativamente a quelle norme imperative che vietano non già direttamente determinati trattamenti, bensì che – esattamente come abbiamo argomentato a proposito dell'art. 5 dell'AI Act - vietano determinate attività le quali *presuppongono necessariamente e tipicamente* determinati trattamenti.

Nel caso dei divieti dell'art. 5 AIA, si trattava di divieti relativi alla immissione sul mercato, messa in servizio ed uso di sistemi di IA, ma non c'è motivo di limitare l'analisi alle disposizioni dell'AIA, perché ci sono trattamenti automatizzati di dati personali, compresi trattamenti automatizzati di dati personali effettuati da sistemi di IA, che possono essere necessariamente e tipicamente presupposti da, in quanto strumentali e finalizzati alla realizzazione di, *attività vietate da altre normative*. Come detto, si tratta di riconoscere in linea di principio che l'esistenza di divieti di certe attività implicanti necessariamente determinati trattamenti debba far ritenere il trattamento in sé considerato illecito *ai sensi del GDPR*.

Possiamo pensare, ad esempio, a piattaforme online che trattano dati personali per giochi d'azzardo o per concorsi a premio *in violazione delle normative nazionali che regolano i giochi d'azzardo e i concorsi a premio*.

---

[41] Regolamento (UE) 2022/2065 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento dei servizi digitali).

[42] 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.

[43] L'art. 18(1)(c) del regolamento (UE) 2024/900 sulla trasparenza e il targeting della pubblicità politica 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.

[44] L'art. 28(2) DSA vieta ai fornitori di piattaforme online di presentare sulla loro interfaccia pubblicità basata sulla profilazione (come definita nel GDPR) che usa i dati personali del destinatario del servizio se sono consapevoli, con ragionevole certezza, che il destinatario del servizio è minore.

ISSN 2239-8570

A mio avviso non c'è dubbio che anche in simili casi, il relativo trattamento di dati personali dovrà ritenersi illecito *ai sensi del GDPR*, ed anche, naturalmente, se le piattaforme in questione utilizzano sistemi di intelligenza artificiale.

Ed in effetti in casi simili, per cominciare, sicuramente saremmo in presenza della violazione del principio espresso dall'art. 5(1)(b) GDPR per cui i dati personali devono essere *raccolti* per *finalità legittime*. Tanto appurato, non ci saranno motivi per limitare il giudizio di violazione del GDPR al solo trattamento che consiste nella *raccolta* dei dati personali, dovendosi al contrario parlare di illiceità che investe in generale ogni ulteriore trattamento finalizzato alla realizzazione di giochi d'azzardo e concorsi a premio *contra legem*, anche in considerazione del precetto che si legge nella proposizione successiva del medesimo art. 5(1)(b) GDPR, a tenore del quale ogni trattamento successivo alla raccolta deve essere conforme a finalità legittime.

Similmente, ed entrando ora nel campo di applicazione oggi maggiormente attivo tra i sistemi di IA[45], ossia area del marketing, è doveroso prendere con nettezza posizione e riconoscere la sostanziale illiceità, per violazione delle norme imperative della direttiva 2005/29/CE (innanzi **UCPD**) e del DSA, dei trattamenti di dati personali finalizzati alla distorsione comportamentale delle persone attraverso lo sfruttamento delle loro vulnerabilità decisionali[46].

Le pratiche di targeting online poste in essere dai professionisti che sfruttano le vulnerabilità decisionali dei consumatori per ottenere, distorcendo il loro comportamento, determinate risposte, sono illecite ai sensi del divieto generale e dei divieti particolari previsti dall'UCPD contro le pratiche commerciali sleali, ingannevoli e aggressive, così come sono illecite quelle poste in essere sulle interfacce online relativamente a qualunque utente online in violazione dell'art. 25 DSA.

Tutti i trattamenti di dati personali - compresi naturalmente quelli automatizzati e, tra questi, quelli che si avvalgono di sistemi di IA – finalizzati allo sfruttamento di vulnerabilità comportamentali con modalità idonee a ottenere una risposta falsata ossia distorta, in violazione di quelle disposizioni, devono ritenersi sostanzialmente illeciti *anche ai sensi del GDPR*.

Relativamente all'impiego di sistemi di intelligenza artificiale, in tutti i casi come quelli esemplificati in questo paragrafo, sarà, di nuovo, da determinarsi con precisione di volta in volta quali trattamenti relativi allo sviluppo e all'uso di sistemi di IA precisamente dovranno ritenersi illeciti, *sulla base delle circostanze del caso* (se tanto quelli in fase di sviluppo – e quali in particolare - che quelli in fase d'uso, o solo quelli in fase d'uso, e

[45] N. CRISTIANINI, *La scorciatoia*, Il Mulino, Bologna, 2023, p. 36 ss.

[46] Cfr. Commissione europea, "*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), pubblicato sulla Gazzetta Ufficiale dell'Unione Europea del 29.12.2021; risoluzione del Parlamento europeo del 12 dicembre 2023, sulla «progettazione dei servizi online che creano dipendenza e sulla tutela dei consumatori».

ISSN 2239-8570

quali in particolare) ma, dal punto di vista generale, credo che non possa dubitarsi dell'esistenza di un livello di potenziale illiceità di trattamenti di dati personali *ai sensi del GDPR* nel contesto di sistemi di intelligenza artificiale sia per trattamenti direttamente vietati che relativamente al caso di sistemi di IA impiegati per attività *contra legem*, come quelle esemplificate, e come tante altre possono immaginarsi, che presuppongono necessariamente e tipicamente determinati trattamenti.

4. L'inidoneità delle condizioni di cui agli artt. 6(1) e 9(2) GDPR a costituire *in concreto* valide basi per il trattamento lecito di dati personali a fronte di norme imperative che vietano direttamente o indirettamente determinati trattamenti.

Come detto ed argomentato *supra*, l'ordinamento prevede divieti diretti ed indiretti di trattamento dei dati personali. Nel primo caso, si tratta di norme imperative che vietano direttamente ed espressamente determinati trattamenti di dati personali. Nel secondo caso, si tratta di norme imperative che vietano determinate attività le quali presuppongono necessariamente determinati trattamenti di dati personali. In tutti questi casi, i trattamenti in questione dovranno ritenersi illeciti.

Deve ora aggiungersi che, in simili circostanze, nessuna delle condizioni astrattamente invocabili ex art. 6 GDPR può effettivamente ed in concreto costituire una valida base per un trattamento lecito.

Ed infatti, quando si dovesse invocare la base del consenso[47], dovrà ritenersi che in simili circostanze si tratterà di un consenso prestato *per* una specifica finalità di trattamento *illegittima*[48]. E quando si dovesse invocare la base dell'esecuzione del contratto[49], dovrà ritenersi che si tratterà dell'esecuzione di un contratto *illecito*. Né, per lo stesso motivo, potrebbe invocarsi validamente la base dell'interesse legittimo[50] o quella dell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri[51].

Il giudizio implicato andrà svolto *in concreto*, come giudizio circa l'idoneità di una base astrattamente idonea, ad essere tale anche in concreto, avuto riguardo al suo profilo di liceità che possiamo perciò definire '*sostanziale*' per distinguerlo da un profilo '*formale*', che si ferma alla ricorrenza o meno di una base astrattamente idonea. Alla stregua di un giudizio sulla liceità sostanziale del trattamento, dovrà concludersi nel senso di dichiarare l'illiceità *ai sensi del GDPR* tutte le volte che, come detto, il trattamento risulti direttamente vietato dalla legge, o necessariamente e tipicamente strumentale al compimento di un'attività vietata dalla legge.

[47] Art. 6(1)(a) GDPR.
[48] S. ORLANDO, *Consenso al trattamento e liceità*, in *Pers. merc.*, 2024, p. 333 ss.
[49] Art. 6(1)(b) GDPR.
[50] Art. 6(1)(f) GDPR.
[51] Art. 6(1)(e) GDPR.

ISSN 2239-8570

5. Giustificazione funzionale e conformità ordinamentale di ciascuna delle basi del trattamento.

A ben vedere, ciascuna delle basi del trattamento lecito dei dati personali previste nell'art. 6(1) GDPR e nell'art. 9(2) GDPR ha una giustificazione funzionale ed un carattere di conformità ordinamentale, incompatibili con la violazione di norme imperative, sicché, alla domanda che abbiamo formulato nel paragrafo 2 *retro* – allorché abbiamo delineato la prima grande questione interpretativa da sciogliere relativamente ai sistemi di IA - dobbiamo dare senz'altro una risposta positiva, che si applica a tutti i casi di trattamento dei dati personali, ossia non limitatamente ai trattamenti inerenti allo sviluppo ed uso di sistemi di IA.

Nel par. 2 ci chiedevamo se il requisito di liceità del trattamento - ricavato dal principio espresso nell'art. 5(1)(a) GDPR[52] - possa interpretarsi nel senso di riferirlo non soltanto alla necessaria presenza di una delle condizioni (o 'basi') per il trattamento di cui all'art. 6(1) GDPR, ma anche nel senso generale di rispetto di norme imperative, e, in questo caso, se si debba avere in considerazione il solo diritto unitario o anche il diritto nazionale applicabile.

Come già accennato *supra*, e come riassumeremo nuovamente qui di seguito, l'esame di ciascuna delle basi dell'art. 6(1) GDPR e di quelle dell'art. 9(2) GDPR consente di dire che in realtà il rispetto o non violazione delle norme imperative del diritto dell'Unione e nazionale applicabile sia necessario *proprio per il rispetto di ciascuna delle medesime basi*.

Cominciando da quella del consenso di cui all'art. 6(1)(a) GDPR, come anticipato sopra (v. *retro* parr. 2 e 4) ed argomentato diffusamente in altri scritti[53], nella formula usata dal legislatore europeo deve ritenersi senz'altro sottintesa l'aggettivazione «legittime» dopo le parole «specifiche finalità» («l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità *legittime*»), in quanto le norme del GDPR *impongono* un'interpretazione di questo tipo. Ed infatti, come già 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 nell'erigendo diritto dei dati inteso a governare l'economia e l'industria dei dati, prendono atto dell'esigenza di regolare l'utilizzazione e la produzione dei dati digitali, ed interpretano questa esigenza *proibendo direttamente o indirettamente determinati trattamenti di dati personali nei più vari settori*.

[52] 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»);[…]".

[53] S. ORLANDO, *Consenso al trattamento e liceità*, cit.; ID., *Il coordinamento tra la direttiva 2019/770 e il GDPR. l'interessato-consumatore*, in *Pers. merc.*, 2023, 222 ss.; ID., *Per un sindacato di liceità del consenso privacy*, *Pers. merc.*, 2022, 527 ss.

Similmente, non sembra potersi dubitare che la base dell'esecuzione del contratto di cui all'art. 6(1)(b) GDPR debba interpretarsi nel senso che la relativa formula sottintenda l'aggettivazione «lecito» dopo la parola «contratto» («il trattamento è necessario all'esecuzione di un contratto *lecito* di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso»), perché davvero non si vede come potrebbe ritenersi essere in concreto una valida base di lecito trattamento dei dati personali la finalità di esecuzione di un contratto illecito.

La successiva base, statuita dall'art. 6(1)(c) GDPR indica in modo evidente (senza bisogno di enunciare in via ermeneutica aggettivazioni sottintese, come nei primi due casi) sia la giustificazione funzionale che il carattere di conformità ordinamentale proprî di tutte le basi: «il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento», dove la funzione è evidente così come la conformità ordinamentale operata attraverso il doveroso rinvio alla totalità dell'ordinamento - nella sua composizione di diritto dell'Unione e nazionale applicabile - per verificare in concreto la presenza (o l'assenza) di un «obbligo legale».

Anche la base dell'art. 6(1)(d) GDPR indica tanto la giustificazione funzionale che il carattere di conformità ordinamentale, posto che, alla stregua della Carta dei diritti fondamentali dell'Unione europea, così come alla stregua delle disposizioni di rango costituzionale di tutti gli ordinamenti degli Stati membri, non è dubitabile che «la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica» costituisca (*melius*: debba costituire) una lecita base di trattamento dei dati personali.

Anche le ultime due condizioni ex art. 6(1)(e) e 6(1)(f) GDPR indicano a ben vedere tanto la giustificazione funzionale che il carattere di conformità ordinamentale, di cui stiamo discorrendo, posto che, come già osservato, è sicuramente errato invocare in concreto la base dell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e quella del legittimo interesse relativamente a trattamenti direttamente o indirettamente vietati dalla legge. Come già ricordato, proprio relativamente alla disposizione di cui all'art. 6(1)(f) GDPR sul legittimo interesse, la CGUE, in una recente sentenza ha espressamente dichiarato che "*Sebbene detta disposizione non esiga che un interesse siffatto sia determinato dalla legge, essa richiede che il legittimo interesse invocato sia lecito*"[54].

Infine, i concetti di cui sopra sono confermati anche nella disciplina della speciale categoria dei dati personali di cui all'art. 9(1) GDPR, laddove le basi per il trattamento in deroga al divieto di cui al primo paragrafo dell'art. 9 esprimono tutte sia la giustificazione funzionale che la conformità ordinamentale delle basi del trattamento di tali speciali categorie di dati, in

[54] Corte di Giustizia dell'Unione europea, Nona sezione, sentenza del 4 ottobre 2024 nella causa C-621/22. In un altro passaggio della medesima sentenza così si legge "[…] un interesse commerciale del titolare del trattamento […] potrebbe costituire un legittimo interesse, ai sensi dell'articolo 6, paragrafo 1, primo comma, lettera f) GDPR, purché non sia contrario alla legge. Spetta tuttavia al tribunale nazionale valutare, caso per caso, l'esistenza di un interesse del genere, tenendo conto del quadro giuridico applicabile e di tutte le circostanze del caso".

ISSN 2239-8570

particolare segnalandosi che nel caso del «consenso esplicito» ivi previsto (art. 9(2)(a) GDPR[55]) la conformità ordinamentale è espressamente enunciata dal legislatore europeo sotto forma di inidoneità del consenso esplicito a vincere il divieto di cui al paragrafo 1 a fronte di norme dell'Unione o nazionali che vietino in modo inderogabile il trattamento di tali dati personali: «*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*».

La riserva di conformità ordinamentale del consenso esplicito *espressamente* prevista dall'art. 9(2)(a) GDPR conferma ciò che è richiesto generalmente dagli artt. 5(1)(a) e 5(1)(b) GDPR, ossia che il Regolamento apre una finestra con vista fuori da sé stesso, *imponendo* all'interprete di guardare fuori dal GDPR.

Allo stesso modo, può osservarsi come l'art. 9(1)(b) GDPR imponga un controllo di conformità ordinamentale relativamente al diritto del lavoro applicabile, nel rispetto delle garanzie fondamentali del lavoratore interessato[56].

6. La liceità *sostanziale* del trattamento e sua distinzione dalla liceità *formale*. Esempi di trattamenti che superano il test di liceità formale ma non quello di liceità sostanziale.

Tutte queste considerazioni sospingono verso la distinzione tra un giudizio di liceità in senso formale, conseguente ad un controllo procedurale sulla ricorrenza di una base astrattamente idonea per il trattamento dei dati personali, ed un giudizio di liceità in senso sostanziale, conseguente ad un controllo di conformità ordinamentale della base in concreto. Il primo giudizio può concludersi nel senso di far ritenere *illecito* un determinato trattamento di dati personali in *difetto* di una base anche solo astrattamente idonea. Il secondo giudizio è solo eventuale, ma al contempo è necessario, nel caso in cui il primo abbia dato esito positivo, ossia nel caso in cui il primo test abbia riscontrato la ricorrenza di una base in astratto idonea ai sensi del GDPR. Esso è volto a quel punto a stabilire se un determinato trattamento di dati personali di cui si sia riscontrata la ricorrenza di una base astrattamente idonea (test di liceità in senso formale) sia, alla stregua di una valutazione *in concreto*, ammesso dall'ordinamento. Il giudizio di liceità sostanziale è perciò volto a verificare che il singolo trattamento non sia

[55] Art. 9(2)(a) GDPR: "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; […]".

[56] Art. 9(2)(b) GDPR: "2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: […] b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; […]".

ISSN 2239-8570

vietato da una norma imperativa dell'Unione o nazionale che proibisca direttamente il trattamento in questione o che vieti un'attività che presuppone necessariamente e tipicamente il trattamento in questione.

Ove si dovesse riscontrare un divieto siffatto, come argomentato *supra* (v. parr. 4 e 5 *supra*), nessuna delle basi di cui all'art. 6(1) o 9(2) GDPR può ritenersi validamente invocabile, ed il trattamento dovrebbe ritenersi illecito ai sensi del GDPR.

Ciò in quanto, come si è provato a dimostrare sopra, tutte le condizioni previste come basi di un trattamento lecito dall'art. 6(1) o 9(2) GDPR hanno una giustificazione funzionale e un carattere di conformità ordinamentale.

Possiamo fare adesso qualche esempio di test che *superano* il giudizio sulla liceità formale ma *non* anche quello sulla liceità sostanziale.

6.1. Primo esempio: sistema di IA di marketing online che impiega algoritmi idonei a distorcere il comportamento delle persone fisiche causando loro un danno significativo.

Sistemi di IA di marketing online possono richiedere ed ottenere il consenso da parte di utenti, in ipotesi anche consensi con tutti i caratteri dell'art. 4, n. 11 GDPR, ed anche consensi espliciti ai sensi dell'art. 22(2)(c) GDPR. Ciononostante, se i sistemi di IA di marketing in questione, impiegano algoritmi idonei a distorcere il comportamento delle persone fisiche causando loro un danno significativo ex art. 5(1)(a) AIA o art. 5(1)(b) AIA, sicuramente i trattamenti di dati personali realizzati per lo sviluppo e l'uso di tali sistemi devono essere sottoposti ad un giudizio di liceità sostanziale, e tipicamente sarà possibile predicare l'illiceità *ai sensi del GDPR* di una serie di trattamenti di dati personali relativamente a questa tipologia di sistemi di IA, derivata dai divieti di immissione sul mercato, messa in servizio ed uso degli stessi posti dall'AIA.

6.2. Secondo esempio: sistema di IA di marketing online che impiega algoritmi idonei a distorcere il comportamento delle persone fisiche senza causare loro un danno significativo

Sistemi di IA di marketing online possono richiedere ed ottenere il consenso da parte di utenti, in ipotesi anche consensi con tutti i caratteri dell'art. 4, n. 11 GDPR, ed anche consensi espliciti ai sensi dell'art. 22(2)(c) GDPR. Ciononostante, se i sistemi di IA di marketing in questione, impiegano algoritmi idonei a distorcere il comportamento delle persone fisiche, sicuramente i trattamenti di dati personali realizzati per lo sviluppo e l'uso di tali sistemi devono essere sottoposti ad un giudizio di liceità sostanziale, e tipicamente sarà possibile predicare l'illiceità *ai sensi del GDPR* di una serie di trattamenti di dati personali relativamente a questa tipologia di sistemi di IA, derivata dai divieti di pratiche commerciali sleali, ingannevoli e aggressive posti dall'UCPD.

ISSN 2239-8570

6.3. Terzo esempio: sistema di IA di marketing politico online che impiega algoritmi che profilano le persone fisiche sulla base delle speciali categorie di dati personali dell'art. 9(1) GDPR

Sistemi di IA di marketing politico online possono richiedere ed ottenere il consenso da parte di utenti, in ipotesi anche consensi con tutti i caratteri dell'art. 4, n. 11 GDPR, ed anche consensi espliciti ai sensi dell'art. 22(2)(c) GDPR. Ciononostante, se i sistemi di IA di marketing in questione, impiegano algoritmi che profilano le persone fisiche sulla base delle speciali categorie di dati personali dell'art. 9(1) GDPR, sicuramente i trattamenti di dati personali realizzati per lo sviluppo e l'uso di tali sistemi devono essere sottoposti ad un giudizio di liceità sostanziale, e tipicamente sarà possibile predicare l'illiceità *ai sensi del GDPR* di una serie di trattamenti di dati personali relativamente a questa tipologia di sistemi di IA, derivata dal corrispondente divieto di cui all'art. 18(1)(c) del regolamento (UE) 2024/900 sulla trasparenza e il targeting della pubblicità politica[57].

7. Adeguatezza del giudizio di liceità sostanziale al suo oggetto: il carattere analitico del test di liceità sostanziale in concreto con riferimento ai singoli trattamenti e ai singoli algoritmi

Il giudizio di liceità sostanziale in concreto deve essere svolto con modalità idonee a valutare in modo analitico i trattamenti automatizzati in relazione ai singoli algoritmi che servono granularmente le miriadi di finalità dei trattamenti.

Un compito di questo tipo richiede necessariamente un salto di qualità di tipo tecnologico da parte delle autorità di controllo, non assolvendo il quale il giudizio richiesto dalla legge non potrà essere adeguato al suo oggetto.

Pertanto si tratta non soltanto di convenire circa la doverosità dell'interpretazione centrata sul criterio dell'adeguatezza del giudizio di liceità al suo oggetto, ai fini di una corretta applicazione del GDPR, ma anche di attrezzarsi tecnologicamente per l'assolvimento del relativo compito.

---

[57] Art. 18(1) del regolamento (UE) 2024/900 relativo alla trasparenza e al targeting della pubblicità politica: "1. Le tecniche di targeting o di consegna del messaggio pubblicitario in ambito di pubblicità politica online che comportano il trattamento dei dati personali sono consentite solo se sono soddisfatte le condizioni seguenti:
a) il titolare del trattamento ha raccolto i dati personali presso l'interessato;
b) l'interessato ha prestato il proprio consenso esplicito ai sensi dei regolamenti (UE) 2016/679 e (UE) 2018/1725 al trattamento separato dei dati personali a fini di pubblicità politica; e
c) tali tecniche non comportano la «profilazione» quale definita all'articolo 4, punto 4), del regolamento (UE) 2016/679 e all'articolo 3, punto 5), del regolamento (UE) 2018/1725 utilizzando le categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679 e all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725".

8. La distribuzione delle competenze e il coordinamento delle attività tra autorità amministrative e giurisdizionali

Tutte le volte in cui il giudizio di liceità del trattamento dei dati personali supera il controllo procedurale sulla ricorrenza di una base astrattamente idonea, si pone il problema di chi abbia competenza per stabilire la conformità ordinamentale del trattamento.

Mentre il primo controllo è sicuramente di competenza delle autorità di controllo nazionali istituite ai sensi dell'art. 51 GDPR (di seguito anche **DPA**, acronimo di *Data Protection Authorities*), è da capire di chi sia la competenza per il secondo controllo.

La stessa questione, naturalmente, coinvolge l'EDPS per quanto riguarda le competenze attribuitegli dall'EUDPR relativamente ai trattamenti fatti dalle istituzioni, gli organi e gli organismi UE.

Il problema fondamentale consiste nello stabilire se le DPA/l'EDPS abbiano sempre e in via generale la competenza di svolgere *autonomamente* il controllo di conformità ordinamentale dei trattamenti dei dati personali, necessario per il giudizio di liceità sostanziale richiesto dal GDPR/EUDPR.

La questione è molto delicata. Essa tocca innanzitutto i confini delle competenze tra le DPA o l'EDPS, da un lato, e, dall'altro lato, le numerose autorità amministrative indipendenti istituite ai sensi del diritto dell'Unione e nazionale nei più vari settori dell'ordinamento, nei quali, come visto, si trovano numerosi divieti diretti e indiretti di trattamento dei dati personali.

Se, per fare un esempio, il trattamento in questione riguarda lo sviluppo e/o l'uso di sistemi assoggettati ai divieti dell'art. 5 AIA, possono le DPA valutare esse stesse autonomamente la ricorrenza, nei sistemi di IA, dei caratteri rilevanti ai fini dei divieti dell'art. 5 AIA?[58]

La questione tocca anche il rapporto tra le DPA/l'EDPS e le autorità giurisdizionali, i cui accertamenti, pure, possono essere necessari per stabilire la conformità ordinamentale di un determinato trattamento in concreto, al fine di giudicarne la liceità sostanziale. Per fare un esempio, si può pensare alla base dell'esecuzione del contratto di cui all'art. 6(1)(b) GDPR: se il primo controllo procedurale fatto da una DPA/l'EDPS ha dato esito positivo rinvenendo l'occorrenza di questa condizione astrattamente idonea come base per un trattamento lecito (i.e. il trattamento serve per l'esecuzione di un contratto), chi ha la competenza per il controllo di conformità ordinamentale successivo, volto ad escludere che si tratti in concreto di un contratto illecito? Questa è generalmente l'area degli accertamenti delle autorità giurisdizionali. E tuttavia, come abbiamo argomentato, è necessario e doveroso *ai sensi del GDPR/EUDPR* proporsi

[58] Relativamente a questo specifico esempio, all'EDPS è attribuita competenza per irrogare le sanzioni amministrative pecuniare alle istituzioni, organi e organismi dell'Unione per la violazione dell'AI Act (art. 100 AIA), inclusa la violazione dell'art. 5 AIA (art. 100(2) AIA). Pertanto, deve ritenersi che sicuramente l'EDPS ha competenza a verificare se i sistemi di IA ricadono tra quelli sottoposti ai divieti dell'art. 5 AIA *anche per l'accertamento della violazione del l'EUDPR* per trattamento illecito dei dati personali impiegati da istituzioni, organi e organismi dell'Unione per lo sviluppo o l'uso di tali sistemi di IA. Torneremo sul punto nel paragrafo 10 *infra*.

ISSN 2239-8570

questo accertamento, perché non può ritenersi una base idonea al trattamento dei dati personali l'esecuzione di un contratto illecito. Il trattamento di dati personali posto in essere per l'esecuzione di un contratto illecito, deve ritenersi illecito *ai sensi del GDPR/EUDPR*.

Il tema ha portata generale, come pure abbiamo argomentato, perché *per ogni base* deve effettuarsi non solo un controllo procedurale sulla ricorrenza di una condizione astrattamente idonea per un trattamento lecito (liceità formale) ma anche un controllo sostanziale in concreto per stabilire se il trattamento non violi in concreto norme imperative dell'ordinamento (diritto dell'Unione e diritto nazionale applicabile) che direttamente o indirettamente lo proibiscono (v. *retro*, par. 5 in particolare).

La doverosità, *in base al GDPR/EUDPR*, di un simile controllo di conformità ordinamentale, in che consiste il giudizio di liceità sostanziale sui trattamenti dei dati personali, propone perciò il tema dell'interpretazione sistematica delle normative che dispongono direttamente o indirettamente i divieti di trattamento, nel senso detto, da un lato, e del GDPR/EUDPR, dall'altro lato.

Nell'impostare questo problema, bisogna innanzitutto considerare che le DPA/l'EDPS[59] hanno la competenza ed il dovere di presidiare all'applicazione del GDPR/EUDPR - *e che dunque si tratta di una competenza limitata a quest'ambito dell'ordinamento* - ma anche tornare a sottolineare che il controllo di conformità ordinamentale è autorizzato e perciò stesso è *imposto dallo stesso GDPR/EUDPR*, e che – dunque - le autorità di controllo proprio esercitando i poteri di loro competenza, *devono* proporsi la questione della liceità sostanziale. Ed infatti, come abbiamo argomentato nei paragrafi precedenti, gli artt. 5(1)(a), 5(1)(b), 6(1), 9(2) del GDPR richiedono di effettuare un test di liceità sostanziale, ossia un controllo sulla conformità del trattamento dei dati personali alle norme imperative del diritto dell'Unione e del diritto nazionale applicabile. In sintesi, come abbiamo detto nei paragrafi che precedono e anche in altra sede[60], il GDPR apre una finestra con vista fuori di sé stesso. E lo stesso fa l'EUDPR attraverso le corrispondenti disposizioni, contenute negli artt. 4(1)(a), 4(1)(b), 5, 10(2) EUDPR. Le autorità di controllo e l'EDPS non possono ignorare questa finestra, perché se la ignorassero violerebbero, rispettivamente, il GDPR e l'EUDPR. Invece: che siano le DPA e l'EDPS a poter e dover guardare fuori della finestra per effettuare *autonomamente* il controllo di conformità ordinamentale necessario per il giudizio di liceità sostanziale, questa è un'altra questione, che attiene ai confini delle loro competenze.

Si tratta in altre parole di capire *come* le autorità di controllo/l'EDPS possono assolvere al compito di considerare nel loro giudizio sulla liceità del trattamento dei dati personali il controllo sulla conformità ordinamentale, mentre non può esserci alcun dubbio che esse abbiano questo compito.

Da qui la complessità del tema.

---

[59] E l'EDPS, relativamente ai trattamenti fatti dalle istituzioni, gli organi e gli organismi UE ai sensi dell'EUDPR.

[60] S. ORLANDO, *Consenso al trattamento e liceità*, cit., p. 353.

ISSN 2239-8570

In alcuni casi, come vedremo, le fonti che prevedono direttamente o indirettamente divieti di determinati trattamenti, aiutano l'interprete ad orientarsi, ma non c'è dubbio che si tratti di un tema di carattere generale. Esso può impostarsi raffigurandosi la necessità di una interpretazione sistematica tra le più diverse fonti dell'ordinamento che governano il contemporaneo diritto dei dati.

L'interpretazione sistematica è necessaria per impostare e risolvere essenzialmente due problemi: non solo quello, a cui si è già accennato, del coordinamento tra le attività di autorità giurisdizionali e amministrative in base alle relative competenze, ma anche quello eventuale della c.d. doppia sanzione.

Senza poter espandere l'analisi in questa sede, direi che il primo è sempre un problema reale, mentre il secondo è un problema eventuale e sovente anche soltanto apparente, perché, in linea generale, la sanzione (se prevista anche nella normativa che prevede, o da cui si ricava, lo specifico divieto di trattamento) non deve in linea di principio ritenersi doppia rispetto a quella prevista dal GDPR/EUDPR, dovendosi in proposito e in senso contrario riconoscere che la fonte normativa che pone o presuppone lo specifico divieto può prevedere sanzioni (e/o altre conseguenze, es. invalidità di atti, e altri rimedi) per contrastare un *comportamento illecito* posto in essere attraverso il trattamento illecito di dati personali, mentre il GDPR/EUDPR sanziona il *trattamento illecito* dei dati personali.

Nella recente disciplina sul marketing politico online, recata dal regolamento (UE) 2024/900[61], i due problemi sono risolti direttamente dal legislatore europeo prevedendosi che per quanto attiene all'inosservanza degli obblighi posti dagli artt. 18 e 19 di quel regolamento in materia di targeting online, si rinvia al potere delle autorità di controllo di cui al GDPR e all'EUDPR di imporre sanzioni pecuniarie «nei limiti delle loro competenze» e si prevede che le sanzioni pecuniarie siano «in linea» con quelle previste dalle disposizioni del GDPR e dell'EUDPR e a concorrenza degli importi massimi ivi previsti (art. 25(5) e (6) regolamento (UE) 2024/900). Tale disposizione, da un lato, elimina in radice l'eventualità di una doppia sanzione, ma dall'altro lato rende necessario accogliere la tesi qui proposta, perché deve riconoscersi che la precisazione «nei limiti delle loro competenze» sta a significare che deve necessariamente riconoscersi essere una specifica e precipua competenza delle DPA degli Stati membri (ai sensi del GDPR) e dell'EDPS (ai sensi dell'EUDPR) quella di sanzionare *in quanto illeciti ai sensi del GDPR e dell'EUDPR* i trattamenti dei dati personali *realizzati in violazione delle norme imperative speciali che pongono i divieti di trattamento* di cui agli artt.18 e 19 del regolamento (UE) 2024/900.

Per quanto riguarda la legge 123/2023 sull'oblio oncologico, l'art. 5(4) della medesima legge, prevede che il Garante privacy vigili sull'applicazione della medesima legge. Questa previsione afferma la competenza dell'autorità garante per la protezione dei dati personali di accertare l'illiceità di qualsiasi trattamento di dati personali realizzato in

[61] Regolamento (UE) 2024/900 relativo alla trasparenza e al targeting della pubblicità politica.

ISSN 2239-8570

violazione degli artt. 2, 3 o 4 della medesima legge. Ma, con ciò stesso, ritengo che il Garante privacy possa accertare e debba dichiarare e sanzionare anche l'illiceità *sostanziale* di ogni simile trattamento *ai sensi del GDPR.*

9. (segue) L'esempio del Sig. Leon

Da quanto sopra esposto si comprende come sia errato ritenere sufficiente il controllo procedurale sulla ricorrenza di una condizione astrattamente idonea a servire da base al trattamento. Tale controllo, propedeutico ad un giudizio di liceità in senso formale, è sufficiente solo quando dia esito negativo (assenza di una base in astratto, con conseguente giudizio di illiceità) ma non quando dia esito positivo (ricorrenza di una base in astratto). In questo caso, come sopra argomentato, è necessario un supplemento di giudizio (giudizio di liceità in senso sostanziale), che si basa su un controllo di conformità ordinamentale in concreto, ossia un controllo volto ad accertare il rispetto o la non violazione delle norme imperative che vietano direttamente o indirettamente determinati trattamenti.

Come pure abbiamo detto, il controllo sulla conformità ordinamentale del trattamento dei dati personali, propedeutico al giudizio di liceità sostanziale, è richiesto dallo stesso GDPR/EUDPR, e tale richiesta pone delicate questioni sulla competenza delle DPA/dell'EDPS relativamente agli accertamenti da svolgersi ai sensi delle normative *diverse dal GDPR o dall'EUDPR*, che prevedono o da cui si ricavano i divieti di trattamento di dati personali rilevanti ai fini del giudizio di liceità sostanziale.

Nelle Linee guida EDPB 8/2020 sul *targeting* degli utenti di social media, versione 2.0 del 13 aprile 2021, si trova l'esempio del signor Leon, destinatario di pratiche di raccolta di dati personali in grado di individuare le persone impulsive e di basso reddito, e dell'impiego di algoritmi che su questa base decidono che persone come lui – ossia persone (ritenute) impulsive e di basso reddito - sono il bersaglio ideale di pubblicità di scommesse online[62].

[62] 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 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'attivita online del signor Leon sui suoi molteplici dispositivi, ossia sul computer portatile, sul cellulare e sul desktop. Sulla base di tale attività e di tutte le informazioni fornite dal signor Leon, il fornitore di social media deduce che sara 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

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 utilizzare i suoi dati personali per bersagliarlo in questo modo[63].

Se facciamo emergere il profilo del controllo di liceità sostanziale del trattamento, 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 vulnerabilità* del Sig. Leon, è da ritenersi senz'altro illegittima perché in contrasto con il divieto generale previsto dall'art. 5 della UCPD (la direttiva 2005/29/CE sulle pratiche commerciali scorrette) e quello delle pratiche commerciali aggressive, in particolare[64].

---

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).

[63] Le Linee guida 8/2020 in commento ((versione 2.0 del 13 aprile 2021) proseguono così argomentando a pp. 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».

[64] V. par. 3 *retro*, ove riferimenti anche alla 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) e alla risoluzione del Parlamento europeo del 12 dicembre 2023, sulla «progettazione dei servizi online che creano dipendenza e sulla tutela dei consumatori». Sembra anche significativo osservare come il profilo funzionale sulle specifiche finalità di trattamento sia stato ritenuto rilevante

Pertanto l'eventuale consenso privacy del Sig. Leon, anche se esplicito ex art. 22 GDPR, deve ritenersi invalido in quanto illecito, perché prestato per una specifica finalità illegittima[65]. Ossia, si deve concludere che nel caso specifico il consenso esplicito del Sig. Leon si rivela, alla stregua di un controllo di conformità ordinamentale, inidoneo a costituire una valida base per il lecito trattamento dei dati personali, perché tipicamente e necessariamente strumentale alla violazione di un divieto (il divieto di porre in essere pratiche commerciali sleali) posto da una norma imperativa dell'Unione europea.

Ha dunque sbagliato l'EDPB? Come detto sopra, quando si deve giudicare la liceità di un determinato trattamento *in concreto*, è un errore fermarsi al giudizio sulla liceità in senso formale, che consiste nell'accertamento della ricorrenza di una condizione astrattamente idonea al trattamento. L'EDPB in quel documento non ha formulato un giudizio *su un caso concreto* ma ha inteso fornire delle istruzioni per formulare giudizi di liceità del trattamento. In questo senso, in quelle Linee guida, l'EDPB avrebbe potuto dire in termini generali che ogni istruzione o indicazione, contenute nelle medesime Linee guida, sulle condizioni da osservarsi per assicurare la ricorrenza di una base astrattamente idonea al trattamento, deve intendersi fornita *con riserva* di verifica in concreto anche della non violazione o del rispetto delle norme imperative del diritto dell'Unione o del diritto nazionale applicabile, che vietano determinati trattamenti.

Nella parte conclusiva della parte delle Linee guida in commento, a proposito dell'esempio del Sig. Leon, dopo l'argomentazione relativa all'art. 22 GDPR[66] così si legge: "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".

---

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».

[65] V. *supra*, parr. 4 e 5 e più diffusamente S. ORLANDO, *Consenso al trattamento e liceità*, cit. *passim*.

[66] "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" (Linee guida 8/2020, versione 2.0 del 13 aprile 2021, p. 29).

ISSN 2239-8570

Si può dunque dire che l'EDPB in queste Linee guida ha esposto una lunga argomentazione avente ad oggetto il controllo procedurale sulla base del trattamento che culmina nel giudizio che ho chiamato in questo scritto di liceità in senso formale, ossia l'individuazione di una base astrattamente idonea; e tuttavia, alla fine, sia pure con una breve frase in coda, l'EDPB ha anche aggiunto che il titolare del trattamento deve condurre una "valutazione caso per caso rispetto alla liceità del trattamento".

Da questo punto di vista, può ritenersi che l'EDPB avrebbe potuto formulare più esplicitamente una riserva alla sua conclusione in punto di liceità del trattamento, nel senso di dichiarare che la sua conclusione era da intendersi sotto riserva di verifica in concreto del rispetto o non violazione di altre norme imperative del diritto dell'Unione e nazionale applicabile, verifica che, effettivamente, rientra in prima battuta tra i doveri del titolare del trattamento, alla stregua del principio di c.d. *accountability* o responsabilizzazione[67].

Si deve anche considerare che l'EDPB avrebbe ecceduto dalle sue stesse competenze ove avesse dichiarato *illecita ai sensi della UCPD* la pratica di targeting dello sfruttamento delle vulnerabilità decisionali presa in considerazione nell'esempio del Sig. Leon.

L'errore dell'EDPB non è stato dunque quello di non fare una affermazione simile (sulla quale non aveva competenza) ma, semmai, quello di non aver esplicitato la riserva del controllo di conformità ordinamentale, nel senso detto.

10. (segue) Il chi e il cosa: la distinzione tra controllo di conformità ordinamentale e giudizio di liceità ai sensi del GDPR (o dell'EUDPR)

Le osservazioni di cui sopra evidenziano ulteriormente il delicato problema delle competenze, di cui si è cominciato a parlare nel paragrafo 8 *supra*, ossia il tema del "chi" e del "cosa" del giudizio di liceità del trattamento, tenuto conto del profilo della liceità in senso sostanziale.

Sulla base di quanto già esposto, il "cosa" del giudizio di liceità *in due fasi* è chiaro, così come la relativa scansione logica. In particolare:

- *Fase [1]* controllo procedurale sulla ricorrenza di una base astrattamente idonea, propedeutico al giudizio di illiceità/liceità in senso formale.
- *Se il controllo sub [1] dà esito negativo*: giudizio di illiceità (chiusura della valutazione).
- *Se il controllo sub [1] dà esito positivo*: la valutazione non si può chiudere, o può chiudersi solo con riserva, perché, per una valutazione definitiva, si rende necessario il controllo e il giudizio *sub Fase [2]*
- *Fase [2]* controllo in concreto di conformità ordinamentale, ossia sul rispetto o non violazione di norme imperative del diritto dell'Unione

[67] Art. 5(2) GDPR, art. 4(2) EUDPR.

ISSN 2239-8570

e nazionale, propedeutico al giudizio di illiceità/liceità in senso sostanziale.

- *Se il controllo sub [2] dà esito negativo*: giudizio di illiceità (chiusura della valutazione).
- *Se il controllo sub [2] dà esito positivo*: giudizio di liceità (chiusura della valutazione).

Il "chi" è più problematico, non per la *Fase [1]* ma per la *Fase [2]*.

Quanto alla *Fase [1]*, il controllo procedurale e il giudizio di liceità in senso formale sono compiuti sicuramente e sempre dalle DPA/dall'EDPS.

Viceversa, per quanto riguarda l'eventuale *Fase [2]*, bisogna a mio avviso distinguere concettualmente il controllo (di conformità ordinamentale) dal giudizio (di liceità sostanziale) che si basa su quel controllo, perché mentre il giudizio compete sempre ed in ogni caso alle DPA/all'EDPS, per il controllo non ci sono motivi per escludere che le DPA/l'EDPS *possano* o *debbano* avvalersi di controlli di conformità ordinamentale posti in essere da altre autorità amministrative o dall'autorità giurisdizionale sotto forma di provvedimenti o di elementi di provvedimenti (accertamenti).

Relativamente al trattamento dei dati personali per lo sviluppo e l'uso di sistemi di intelligenza artificiale, il problema è stato risolto normativamente dal legislatore europeo per l'EDPS dall'art. 100 AIA, ma non anche per le DPA.

In particolare, poiché l'AI Act ha attribuito all'EDPS competenza ad irrogare sanzioni ai sensi dell'AI Act alle istituzioni, organi e organismi della UE per violazioni dell'AI Act, compreso per violazioni dell'art. 5 AIA (art. 100(2) AIA), sembra corretto ritenere che l'EDPS potrà e dovrà a quel punto utilizzare ogni relativo accertamento anche per dichiarare e sanzionare i trattamenti illeciti dei dati personali *ai sensi dell'EUDPR* relativamente allo sviluppo e/o all'uso dei sistemi di IA assoggettati ai divieti dell'art. 5 AIA.

Diversamente, nessuna indicazione utile in favore di una corrispettiva competenza in favore delle DPA è contenuta nell'AI Act, che rimette agli Stati membri di individuare le autorità di vigilanza del mercato ai sensi del medesimo regolamento (autorità che possono essere perciò scelte dagli Stati membri in autorità diverse dalle DPA)[68].

Se l'Italia non dovesse attribuire competenze specifiche al Garante per la protezione dei dati personali ad agire come autorità di vigilanza del mercato ai sensi dell'AI Act, ogni qual volta si presenterà la questione della valutazione della liceità *ai sensi del GDPR* del trattamento di dati personali per lo sviluppo e/o l'uso di sistemi di IA assoggettati ai divieti dell'art. 5 AIA, si porrà il problema della competenza e dei limiti del Garante privacy italiano rispetto all'accertamento della ricorrenza nel caso di specie dei caratteri rilevanti per qualificare il sistema di IA tra quelli sottoposti ai divieti dell'art. 5 AIA. Lo stesso tema vale generalmente per tutte le DPA istituite ai sensi dell'art. 51 AIA negli altri Stati membri.

[68] Cfr. art. 70 AIA.

ISSN 2239-8570

Ma, naturalmente, il tema del coordinamento e dei confini di competenze tra autorità amministrative e giurisdizionali non riguarda soltanto i divieti dell'art. 5 AIA, poiché esso investe tutti i divieti di trattamento di dati personali posti o ricavabili da norme imperative del diritto dell'Unione e nazionale.

Si tratta di un tema molto ampio e pieno di implicazioni, che necessita di una trattazione specifica ed articolata. Le notazioni e le distinzioni di cui sopra sono offerte per impostarlo nei termini che riteniamo corretti.

11. Conclusioni

Un'ultima considerazione sembra opportuna per calare, per così dire, le interpretazioni che si sono esposte in questo scritto nella realtà incandescente del dibattito attuale sulle basi del trattamento e in particolare su quella del consenso, in contrapposizione a quella dell'esecuzione del contratto e a quella del legittimo interesse.

Come noto, in quel dibattito, sovente viene addebitato ai grandi titolari dei trattamenti digitali dei dati personali la volontà di 'rifugiarsi' (per convenienza delle conseguenze giuridiche) nella base dell'esecuzione del contratto o al più in quella del legittimo interesse, mentre, da parte di coloro che vedono minacciata da queste basi la protezione dei dati personali, quella del consenso viene considerata l'unica 'arma' della privacy, anche se viene al contempo lamentato che si tratta di un'arma effettivamente spuntata[69].

Volendo calare la teoria della liceità sostanziale in questo contesto fortemente contrapposto, per non dire litigioso, ed utilizzando le parole suggestive di 'rifugio' e 'arma' solo per chiarezza di riferimento ai termini di quel dibattito (e senza per ciò stesso esprimere alcun giudizio) mi sembra che si possa dire senza incertezze che, accogliendo quella teoria, la parola 'base' cesserebbe di essere sinonimo di 'rifugio' relativamente all'esecuzione del contratto e al legittimo interesse, perché l'illiceità sostanziale può colpire *tutte* le basi invocate dai titolari per il trattamento (anche quella dell'esecuzione del contratto e del legittimo interesse), e si potrebbe, pertanto, finalmente depotenziare l'aspettativa intorno alla base del consenso, i.e. si potrà riconoscere che si possono e si devono proteggere i diritti fondamentali delle persone *anche* sul piano delle basi dell'esecuzione del contratto e del legittimo interesse. E dunque potrà riconoscersi, anche da parte di coloro che orientano la loro interpretazione esclusivamente alle conseguenze pratiche, che non ci sarà più 'bisogno' di ritenere il consenso come l'unica vera 'arma' della privacy.

[69] La letteratura è molto ampia. Per rassegne aggiornate e ragionate, che tengono conto anche della letteratura straniera e di esperienze di paesi extra UE, cfr. per tutti, I. COFONE, *The Privacy Fallacy. Harm And Power In The Information Society*, Cambridge University Press, Cambridge, 2024; G. MALGIERI, *Vulnerability and Data Protection Law*, Oxford University Press, Oxford, 2023; A.M. GAROFALO, *Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR*, in *Annuario 2021 Osservatorio Giuridico sulla Innovazione Digitale -Yearbook 2021 Juridical Observatory on Digital Innovation*, a cura di S. Orlando e G. Capaldo, Sapienza Università Editrice, Roma, 2022, p. 119 ss.

ISSN 2239-8570

Al contempo, potrà comprendersi come il giudizio di liceità, se svolto in modo corretto, potrà sfatare la credenza che il consenso sia un''arma spuntata'. Ed infatti, il giudizio di liceità, correttamente inteso, potrà essere non limitato alla liceità formale, con la conseguente possibilità di vedere importanti ipotesi di illiceità (sostanziale) che oggi non sono ancora osservate o tematizzate correttamente, promuovendo finalmente un giudizio realisticamente adeguato al suo oggetto, ossia rivolto analiticamente agli algoritmi che realizzano le miriadi di finalità di trattamento effettivamente perseguite dai trattamenti automatizzati.

Ed infatti, per *tutte* le basi, compresa quella del consenso, come detto, l'accertamento della liceità sostanziale in concreto consente e richiede che il controllo di conformità ordinamentale venga svolto capillarmente, ovvero che esso si incentri sui singoli trattamenti e i singoli algoritmi, consentendo esiti valutativi variegati: di liceità per determinati trattamenti e di illiceità per altri trattamenti, granularmente individuati sulla base dei tratti rilevanti per i divieti di trattamento previsti dalle norme di volta in volta considerate. Questo è particolarmente visibile nei sistemi di IA di marketing, nei quali possono riscontrarsi *all'interno dello stesso sistema* algoritmi preordinati a finalità di trattamento legittime (influenza leale) con altri disegnati per servire finalità illegittime (distorsione comportamentale delle persone attraverso lo sfruttamento di determinate vulnerabilità decisionali). In casi simili, molto diffusi nella realtà, si dovrà concludere per l'illiceità (sostanziale) di alcuni trattamenti e la liceità (sostanziale) di altri, quale che sia la base invocata dal titolare del trattamento, ossia a prescindere dal profilo di liceità (formale) attinente alla ricorrenza di una condizione astrattamente idonea a servire come base del trattamento. E con conseguente irrilevanza giuridica delle formule generiche che quasi sempre accompagnano le informative sulle finalità dei trattamenti (es. finalità di marketing, finalità di pubblicità di terze parti etc.).

Se si conviene con la teoria della liceità sostanziale, le due grandi questioni che rimangono aperte sono quella della competenza e quella tecnologica. Come detto, la prima consiste nello stabilire di volta in volta - in base alle norme in questione, ossia quelle rilevanti per il controllo di conformità ordinamentale - se le autorità di controllo e l'EDPS possano, ai fini del giudizio di liceità sostanziale di loro competenza (da condursi alla stregua, rispettivamente, del GDPR e dell'EUDPR) accertare *autonomamente* la conformità ordinamentale dei trattamenti. La seconda, come pure detto, consiste nel dotare le autorità di controllo e l'EDPS di strumenti tecnologici idonei a compiere la loro, o a controllare l'altrui valutazione di conformità ordinamentale in modo capillare per ciascun trattamento, ossia al livello dei relativi algoritmi, in modo da adeguare il giudizio di liceità sostanziale del trattamento al suo oggetto.

ISSN 2239-8570