European Journal of Privacy Law & Technologies

2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

Published Online by G. Giappichelli in June 2019
www.ejplt.tatodpr.eu

AI e GDPR:
L'AUTOMATED DECISION MAKING, LA PROTEZIONE DEI DATI E IL DIRITTO ALLA 'INTELLEGIBILITÀ' DELL'ALGORITMO

Emiliano Troisi

Key-words: AI – automated decision-making – data protection – algorithm disclosure

Category: Legal Area

Topic: Data Protection Law

1. Introduzione

Il Regolamento Generale sulla Protezione dei dati, il Reg. 2016/679/UE, in sigla GDPR, nasce e muove i suoi primi passi in una società digitale e in rapida e continua evoluzione. Tra IoT, Big Data Analytics, machine learning e Intelligenza Artificiale in tutte le sue applicazioni, ogni persona fisica, in ogni momento, è interessata da un trattamento dei propri dati o vi è potenzialmente soggetta. Sistemi di Profilazione e Data Analysis scovano correlazioni tra questi dati, e da questi estrapolano altri dati; predicono comportamenti, carpiscono interessi, intuiscono debolezze. Gli interessati e i loro dati, da oggetto del trattamento ne diventano spesso il 'prodotto'. Sulla base di questo 'prodotto' altri sistemi di IA decidono; a volte sbagliano, e quando sbagliano non è più soltanto la privacy del data-subject ad essere in pericolo ma il suo diritto a non essere

discriminato, ad avere un libero ed equo accesso a beni e servizi, a non essere manipolato a sua insaputa da forme di marketing scorrette, aggressive e invadenti, ma anche la legittima pretesa a contestare le decisioni lesive di una macchina o, soprattutto, a che queste non siano assunte in modo poco trasparente e sulla base, magari, di dati errati e incompleti.

A tutto questo il nuovo Regolamento Privacy risponde con una tutela più ampia e decisa rispetto al passato, una tutela che si estende oltre la mera protezione dei dati e fino a ricomprendere ogni diritto e libertà dell'individuo che possa esserne minacciata; diversa anche la prospettiva: destinatario delle norme è non più chi sia soggetto ad un trattamento del dato ma ogni persona fisica che vi possa essere potenzialmente coinvolta. Ancora, il GDPR introduce i concetti di rischio e accountability: in una società caratterizzata dalla circolazione continua e dinamica dei dati, in cui le modalità del trattamento come pure le sue finalità cambiano continuamente e diventano più complesse, anche la tutela degli interessati, per essere efficace, deve essere dinamica e parametrata, caso per caso, alle specifiche criticità.

Il presente articolo si soffermerà sulla pratica dei trattamenti decisionali automatizzati, o Automated Decision-Making, trattamenti condotti esclusivamente mediante applicazioni di Intelligenza Artificiale e potenzialmente anche molto lesivi della sfera giuridica soggettiva di chi vi sia sottoposto. Se ne individuerà la disciplina prevista nella cornice del GDPR, a partire dalle ridotte ipotesi in cui sono consentiti, i diritti e le specifiche cautele contemplate dal Regolamento, proponendo un'interpretazione ampia e di sistema dell'art. 22 e delle norme ad esso collegate.

Si indugerà, in particolare, sugli specifici e pregnanti oneri informativi posti a carico del titolare del trattamento, tentando di dimostrare come si spingano fino a richiedere una vera e propria '*disclosure*' degli algoritmi decisionali, a beneficio della consapevolezza degli interessati ma anche funzionale ad assolvere specifici obblighi di accountability.

In conclusione un accenno al ruolo sempre più centrale, e di peculiare importanza, che assumono e vanno sempre più assumendo, in questo ambito, la privacy by design e by default.

2. ADM: il divieto generale di trattamenti decisionali automatizzati, eccezioni e condizioni

Come anticipato, il GDPR raccoglie la sfida dell'Intelligenza Artificiale applicata al trattamento dei dati personali rispondendone a tutti i potenziali rischi con la previsione di una disciplina a tutela dei soggetti coinvolti che risulta par-

ticolarmente forte, incardinata su di uno stringente divieto generale di trattamento automatizzato senza consenso e ulteriormente arricchita di speciali misure e oneri informativi a carico del titolare del trattamento – come si vedrà, particolarmente gravosi – e diretti ad assicurare all' interessato il più ampio potere di controllo possibile sull'utilizzo dei propri dati.

L'art. 22 del Regolamento, infatti, espressamente sancisce il diritto dell'interessato a "non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona". Il riferimento è al cosiddetto Automated Decision Making (o più brevemente ADM), ovvero quel fenomeno per cui un sistema informatico programmato per assolvere a una specifica funzione o erogare un certo servizio della società dell'informazione è in grado di assumere, grazie ad un meccanismo inferenziale algoritmizzato – e perciò senza coinvolgimento umano –, una decisione rilevante per i soggetti interessati dalla stessa e basandosi a tal fine unicamente su una valutazione automatizzata dei loro dati personali o una profilazione degli utenti.

Il divieto di ADM, ai sensi del paragrafo 2 dello stesso articolo, non si applica solo se, e nella misura in cui i trattamenti decisionali automatizzati sono necessari per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento oppure siano basati sul consenso dell'interessato.

La possibilità di ricorrere lecitamente a trattamenti di questo tipo è quindi estremamente ristretta: non tutte le circostanze normalmente ammesse dall'art. 6 (1) (a-f) del Regolamento quali base giuridica del trattamento valgono a legittimare il trattamento condotto con meccanismi informatici automatizzati. L'ADM è ammesso solo in presenza di quelle condizioni autorizzative per così dire "consensuali", idonee ad assicurare una più ampia consapevolezza dell'interessato, con la conseguenza che deve ritenersi illegittimo in tutti i casi in cui l'interessato non vi abbia acconsentito espressamente attraverso una propria consapevole manifestazione di volontà, o direttamente [1], o nell'ambito di un più complesso rapporto contrattuale, sul presupposto però, in quest'ultimo caso, che il trattamento automatizzato sia da considerarsi necessario [2] alla conclusione o all'esecuzione dell'accordo.

[1] E per una o più finalità specificamente individuate, ai sensi dell'art. 6 (1) (a) GDPR.

[2] Il paragrafo 2, lett. a) dell'art. 22 GDPR contenente un'esenzione dal generale divieto di ADM deve essere interpretato, in ragione del suo carattere derogatorio, in senso restrittivo e pertanto perché il trattamento decisionale automatizzato possa essere considerato legittimo questo deve risultare, considerate le circostanze del caso, l'unico strumento possibile ovvero l'unico praticamente utilizzabile per raggiungere lo scopo contrattuale. In tal senso anche le *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, n. 251, p.23,* adottate dal Gruppo dell'articolo 29 per la tutela dei dati il 3 ottobre 2017.

In entrambe queste ipotesi in cui il trattamento decisionale automatizzato sia consentito, il titolare del trattamento ha, inoltre, il dovere - ai sensi del paragrafo 3 dell'esaminando art. 22 GDPR - di adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi del *data subject*, e tra questi, in particolare, è tenuto in ogni caso a garantirgli il diritto ad ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestarne la decisione.

Ciò detto, bisogna aggiungere che il GDPR ammette pure che possa essere consentito – ai sensi del paragrafo 2, lett. b) dell'articolo in esame - adottare decisioni sulla base di un trattamento automatizzato in altre singole ipotesi previste da apposita norma autorizzativa del diritto dell'Unione o dello Stato Membro cui è soggetto il titolare del trattamento; ciò eccezionalmente pur in assenza del consenso dell'interessato e sempre che siano, anche qui, adottate misure adeguate alla tutela delle persone fisiche coinvolte. Secondo il Considerando 71 del Regolamento queste ipotesi possono includere, ad esempio, l'utilizzo di trattamenti informatizzati a fini di monitoraggio o prevenzione di frodi od evasione fiscale, ma in ogni caso deve ritenersi necessario – a parere di chi scrive – che il ricorso a tali meccanismi risulti giustificato alla luce del perseguimento di scopi di rilevante interesse pubblico e la relativa compressione dei diritti e delle libertà dei soggetti coinvolti sia proporzionata. In questi casi il Regolamento si limita a prescrivere l'obbligo per il legislatore di prevedere misure adeguate a tutela dei singoli ma il diritto a richiedere l'intervento umano e a contestare eventualmente la decisione non risulta assicurato dal paragrafo 3 dell'art. 22 (come invece negli altri casi esaminati), seppur nulla toglie, ovviamente, che le norme autorizzative di tali trattamenti, nel prevedere le salvaguardie richieste, possano predisporre forme di tutela anche più ampie.

Va infine sottolineato che sono in ogni caso vietati i trattamenti automatizzati e le profilazioni che coinvolgano i dati sensibili di cui all'art. 9 del GDPR, salvo che l'interessato abbia prestato il proprio consenso esplicito o questo sia consentito da apposita base normativa nel diritto dell'Unione o degli Stati Membri e purché il trattamento sia necessario per motivi di interesse pubblico e proporzionato alla finalità perseguita.

(*Segue*). La speciale protezione dei minori d'età

Un ulteriore appunto può farsi in merito ai trattamenti che riguardino minori d'età. L'art. 22 di per se non introduce obblighi diversi né tratta in maniera distinta l'ipotesi in cui l'ADM interessi minori d'età. Sebbene il dettato del Considerando 71, per quanto laconicamente, restituisca una chiara volontà, nelle in-

tenzioni del legislatore europeo, di negare l'ammissibilità di decisioni basate unicamente su trattamenti automatizzato che producano effetti giuridici o comunque incidano significativamente su minori ("Tale misura non dovrebbe riguardare un minore"), tale assunto non è raccolto dalla disposizione regolamentare approvata, con la conseguenza che trattamenti decisionali automatizzati che riguardino minori devono ritenersi leciti nelle medesime ipotesi in cui l'ADM sia consentito per gli adulti a norma del citato paragrafo 2 dell'art. 22 del Regolamento.

La norma tuttavia va contestualizzata e letta nell'ambito delle particolari tutele che in ogni caso, in via generale, il GDPR accorda ai minori che siano interessati da un trattamento dei dati. Il bisogno di una particolare protezione dei minori emerge innanzitutto chiaramente dal Considerando 38 che attesta la necessità di specifiche misure di salvaguardia, specialmente nel caso di raccolta di dati all'atto di servizi informatici offerti direttamente al minore per scopi di profilazione e marketing, in ragione proprio della minor consapevolezza dei rischi e delle conseguenze del trattamento dei propri dati che ci si possa ragionevolmente aspettare da loro per via della tenera età.

In ragione di ciò deve ritenersi quindi fuori di dubbio che il titolare del trattamento debba farsi carico, in caso di trattamenti automatizzati *ex* art. 22, di oneri specifici: ad esempio le misure adeguate a tutela dei diritti e delle libertà dell'interessato richieste dal paragrafo 3 dovranno certamente essere parametrate, in caso di minori, alla speciale protezione evocata nella cornice delle norme europee sulla privacy. Altrettanto pacificamente, nelle ipotesi in cui i trattamenti automatizzati poggino su base consensuale (verosimilmente la stragrande maggioranza dei casi) deve pure farsi applicazione della particolare disciplina di cui all'art. 8 GDPR; questa pone particolari condizioni al consenso al trattamento prestato dai minori, oltre che peculiari oneri di salvaguardia a carico del titolare del trattamento a cagione della speciale vulnerabilità che caratterizza la categoria di interessati in questione. Ove il trattamento di cui all'art. 22, paragrafo 2 si giustifichi in quanto necessario alla conclusione od esecuzione di un contratto tra il minore e il responsabile del trattamento, trovano poi applicazione anche tutte le norme di diritto interno relative alla validità ed efficacia di contratti conclusi dal minore di età [3].

3. Art. 22 del Regolamento: una fattispecie ampia

Orbene, individuati i casi in cui è consentita, a norma del GDPR, l'Automated

[3] Cfr. sul tema, Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, n. 251* del 3 ottobre 2017.

Decision Making e una prima parte della sua disciplina, prima di passare all'esame della rimanente parte delle norme che applicabili - che, come accennato, impongono al titolare del trattamento di predisporre talune salvaguardie tra cui almeno il diritto all'intervento umano, ma anche, per quanto in questa sede maggiormente interessa, del tutto peculiari oneri di trasparenza e informazione che si estendono alla 'logica' dell'algoritmo - è opportuno soffermarsi sulla fattispecie di cui all'art. 22 (1) del Regolamento ed individuare cosa si intenda per (e quindi in quali casi trovi applicazione la disciplina in esame) "decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che [...] riguardano direttamente [l'interessato, ndr] o che incida in modo analogo significativamente sulla sua persona.

Di trattamento automatizzato il Regolamento non dà una precisa definizione, l'art. 22 (1) vi include però espressamente la profilazione. Ai sensi dell'art. 4, per profilazione, nell'ambito del GDPR, si intende qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di questi per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare e prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica". La profilazione è quindi una specie di trattamento automatizzato che consiste nell'esercizio, da parte di un software, un motore inferenziale, di un'operazione deduttiva capace di ricavare cioè da una certa quantità di dati inseriti in un data-set – analizzati e individuate tra loro, automaticamente, delle correlazioni statistiche – altri dati relativi a caratteristiche o schemi comportamentali attribuibili ad un determinato individuo o gruppi di essi al fine di classificarlo/i in precisi gruppi o categorie e/o predirne probabili comportamenti futuri.

Categoria più ampia della profilazione, dunque, per trattamento automatizzato deve intendersi in generale ogni raccolta e analisi di dati personali compiuta automaticamente da un agente informatico programmato a tale scopo.

I trattamenti automatizzati di cui all'art. 22 GDPR rilevano inoltre, espressamente, solo in quanto siano 'decisionali', conducano cioè ad (e applichino) una decisione che influisca sull'interessato. Questo consente di escludere dalla fattispecie tutti quei trattamenti di dati non tipicamente 'inferenziali', in cui cioè l'utilizzo di tecniche informatiche sia limitato, magari, alla conservazione e/od organizzazione di dati personali senza comportare alcun passaggio analitico e/o valutativo degli stessi. Nei trattamenti decisionali automatizzati, invece, i dati sono, al contrario, raccolti (o sottoposti alla macchina) proprio perché questa, eseguendo un dato calcolo, applicando cioè al *data-set* regole deduttive algoritmicamente definite nel programma, li analizzi per arrivare ad una certa 'soluzione', un *output* 'decisionale', appunto.

Questa decisione – perché il relativo trattamento sia rilevante ai fini e per gli

effetti della disposizione in esame, l'art. 22 del Regolamento – deve essere "basata unicamente sul trattamento automatizzato"[4]: interpretazione letterale della disposizione vorrebbe dunque che ricadano nell'ambito applicativo della esaminanda disciplina solo quelle decisioni *fully automated,* dovendosi invece ritenere escluse tutte quelle in cui sia possibile riscontrare un benché minimo coinvolgimento umano che possa variamente 'interferire' col processo decisionale automatizzato, potendo verificare o modificare la decisone ma anche, ad esempio, meramente ratificarla. Un'interpretazione siffatta, a ben vedere, rischierebbe di escludere dall'ambito applicativo della rigorosa disciplina di tutela in esame una buona parte di decisioni che sono in sostanza esito di trattamenti automatizzati ma, ad esempio, formalmente applicate per intervento umano. Molte di queste si prestano anche ad avere effetti potenzialmente molto incisivi sugli interessati; si pensi a tutti i meccanismi di '*scoring*', ampiamente utilizzati nella prassi digitale, ad esempio, per selezionare gli aspiranti ad una posizione lavorativa o valutare la probabile solvibilità di chi miri ad ottenere un fido bancario: non è raro che in questi casi gli interessati siano valutati con strumenti informatici che, applicando ai dati personali funzioni statistiche, assegnino loro un certo valore di merito, uno '*score*' appunto, e che la decisione finale, formalmente spettante ad un funzionario umano sia in realtà meramente passiva, limitandosi magari questo ad abbinare, spesso anche seguendo rigide linee guida predefinite, un certo esito ad un determinato '*score*' senza avere od esercitare alcun potere realmente 'valutativo' [5].

Tutto ciò, altrimenti vanificandosi gli scopi di tutela della esaminanda disciplina, dovrebbe più opportunamente condurre ad adottare un'interpretazione larga dell'art. 22 ritenendo incluse nella fattispecie tutte le 'decisioni automatizzate nella sostanza', anche quelle, cioè, che, benché implicanti nel processo decisionale un qualche intervento umano, questo si configuri come ininfluente rispetto al contenuto della decisione. In tal senso si esprime anche lo stesso Gruppo di Lavoro dell'articolo 29 che espressamente scrive "*The controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing. To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data*" [6].

---

[4] Art. 22 (1) GDPR.

[5] Cfr. G. Malgieri, G. Comandè, *Right to legibility of automated decision-making,* in *International Data Privacy Law,* 2017, vol. 7, n. 4.

[6] Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, n. 251* del 3 ottobre 2017, p. 21.

Prima di esso, registrava un simile orientamento anche il Garante Privacy inglese, l'Information Commissioner's Office (ICO) per cui "*the interpretation of the word "solely" in the context of Article 22(1) [...]is intended to cover those automated decision-making processes in which humans exercise no real influence on the outcome of the decision, for example where the result of the profiling or process is not assessed by a person before being formalized as a decision*" [7].

Ad ogni modo, come pure fa notare qualcuno [8], un indizio a conferma di tale interpretazione può in realtà intravedersi già nello stesso dato letterale del disposto dell'art. 22 (1) GDPR che si riferisce non a decisioni unicamente automatizzate, bensì a decisioni "*basate*" unicamente su trattamenti automatizzati: la sottile conseguenza è potersi facilmente considerare, perciò, volendo, 'letteralmente' incluse anche, quantomeno, quelle decisioni formalmente imputabili ad un agente umano ma in realtà mera applicazione passiva di valutazioni computerizzate [9].

Procedendo nell'interpretazione, queste decisioni, a norma dell'art. 22 (1) del Regolamento, oltre che basate su trattamenti automatizzati, devono pure "produrre effetti giuridici [nei confronti dell'interessato, ndr] o incidere in modo analogo significativamente sulla sua persona". L'effetto di tali decisioni deve dunque influire, negandolo o limitandolo, sul libero esercizio di un diritto della persona riconosciuto dall'ordinamento giuridico. Si pensi, e.g., al diritto a non essere discriminati in una pratica di assunzione online che non preveda intervento umano, applicazione *digital* del, anzi dei, relativi diritti previsti dalla disciplina giuslavoristica. Il catalogo di diritti potenzialmente afflitti da trattamenti decisionali automatizzati si allarga poi notevolmente tenendo da conto che questo abbraccia anche tutti quei diritti fondamentali della persona di rango costituzionale – previsti dalla nostra Costituzione come dalla Convenzione europea dei diritti umani e dalla Carta di Nizza – diritti espressi in forma aperta come la libertà di espressione, la libertà e segretezza della corrispondenza, la libertà di circolazione, di culto, il diritto di difesa e, più di tutti, il principio di non discriminazione: diritti e libertà naturalmente 'elastici', che non costituiscono cioè un *numerus clausus* ma si prestano a coprire tutta una gamma aperta di situazioni giuridiche individuali che possono essere esposte ad un concreto rischio per chi ne sia titolare a fronte di decisioni confliggenti, ed ingiuste, di un'Intelligenza Artificiale [10].

---

[7] Information Commissioner's Office, Feedback request – Profiling and automated decision-making, 2017, 19, richiamato anche in G. Malgieri, G. Comandè, *Right to legibility of automated decision-making*, in *International Data Privacy Law,* 2017, vol. 7, n. 4.

[8] G. Malgieri, G. Comandè, *Right to legibility of automated decision-making*, in *International Data Privacy Law,* 2017, vol. 7, n. 4.

[9] Basate cioè su un dato statistico offerto dalla macchina.

[10] Si ricorda inoltre che la stessa 'libertà informatica', come è stata autorevolmente definita,

Questa tutela ampia dei diritti della persona accordata dall'articolo in esame – e che appunto non si limita affatto al diritto alla riservatezza dei dati [11] – è ulteriormente allargata dal prosieguo della disposizione; il paragrafo 1 dell'art. 22 estende infatti la sua portata anche a quei fenomeni di ADM che pur non intaccando situazioni giuridiche soggettive apertamente qualificate come diritto "incidano [comunque, ndr] in modo analogo e significativamente sulla persona", ovverosia, nell'interpretazione che pare più consona, colpiscano, e gravino profondamente (questo il significato da attribuirsi all'espressione '*significativamente*') su interessi legittimi o comunque legittime pretese della persona umana purché non di mero fatto, ossia situazioni giuridiche che l'ordinamento, benché non riconosca come diritti immediatamente azionabili dall'individuo, ritenga ugualmente degne di protezione o accordandovi una qualche forma di tutela o quantomeno dimostrando un complessivo giudizio di riprovevolezza verso pratiche e comportamenti che ne minaccino il libero e pieno godimento individuale. Questo è il significato che a parere di chi scrive dovrebbe attribuirsi all'espressione "*incidano in modo analogo" (*"*similarly*" nella versione inglese del Regolamento), espressione che merita considerevole attenzione da parte dell'interprete perché assolutamente nuova: è infatti aggiunta *ex novo* dal GDPR accanto all'espressione "*incidano significativamente*" già presente invece nella pregressa formulazione della norma in esame, l'art. 15 dell'abrogata Direttiva 95/46/CE.

L'interpretazione proposta si spiega (e ne risulta corroborata) inoltre anche guardando al contesto politico del Regolamento sulla protezione dei dati e i suoi motivi ispiratori: se da un lato infatti, in modo lungimirante, il GDPR coglie gli enormi rischi per la persona che lo sviluppo e la diffusione di applicazioni di AI e machine learning recano con se – decidendo appunto di prevedere una tutela ampia, estesa ben oltre la privacy e fino a coprire ogni possibile diritto e libertà vulnerabile della persona – dall'altro lato, con altrettanta lungimiranza, non tra-

---

intesa in senso attivo, e cioè come libertà di valersi senza limitazioni, neppure tecnologiche come può essere una decisione automatizzata, degli strumenti informatici al servizio del proprio diritto di comunicare, trasmettere e ricevere informazioni, accedere a servizi telematici, partecipare, insomma, alla società digitale trova un suo radicato fondamento costituzionale ed esprime, per via ermeneutica, nuovi diritti soggettivi, parimenti meritevoli di tutela, da quelli tradizionalmente statuiti opportunamente adattati dall'interprete al rinnovato contesto tecnologico in cui viviamo. Sul punto V. Frosini, *L'Orizzonte giuridico di Internet,* in *Il diritto dell'informazione e dell'informatica*, n. 2, 2002, p. 275; T.E. Frosini, *Tecnologie e libertà costituzionali*, in *Il diritto dell'informazione e dell'informatica*, n. 3, 2003, nonché in *Libertè Egalitè Internet*, Napoli, 2016, p. 19 ss.; ID., *Il diritto costituzionale di accesso a Internet*, in M. Pietrangelo (a cura di), *Il diritto costituzionale di accesso a Internet*, Napoli, 2011, nonché in *Libertè Egalitè Internet*, Napoli, 2016, p. 50 ss.

[11] Che pure è componente essenziale, si ricorda, del rispetto costituzionalmente sancito della libertà individuale e della dignità della persona umana. Sul punto, anche con profili comparati, T.E. Frosini, *Il diritto all'oblio e la libertà informatica,* in *Il diritto dell'informazione e dell'informatica*, n. 4/5, 2012, nonché in *Libertè Egalitè Internet*, Napoli, 2016, p. 120 ss.

scura di cogliere, per converso, l'enorme potenziale espansivo per la società, l'economia e l'informazione che gli stessi strumenti tecnologici schiudono [12]: non è un caso che fin dall'art. 1 del GDPR è scritto che "*il Regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*" ma anche "*relative alla libera circolazione di tali dati*" (pf. 1); ma ancora più significativamente al paragrafo 3, che tale "*libera circolazione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati*". In quest'ottica è ben normale che la tutela, per quanto ampia, riconosciuta dall'art. 22 trovi un limite nella proporzione, nel giusto bilanciamento, cioè, tra il libero utilizzo, nel mercato digitale, di sistemi automatizzati e le contrarie pretese soggettive che per avere tutela, o anzi per meglio dire la tutela 'più forte' di cui all'art. 22 [13] (in deroga a quella comune), è richiesto che siano legittime e, se non qualificate come diritti, quantomeno che l'ordinamento dimostri di proteggerle in modo analogo dal rischio concreto di gravi violazioni ('*significative*', ad usare il linguaggio del Regolamento).

Si lasci chiarire con un esempio; vieppiù afferente una circostanza frequentissima nel digital marketing. Non esiste nell'ordinamento un diritto a non ricevere *targeted advertising* [14], una forma cioè di marketing '*tailored*' basato sulla profilazione. Questa è una pratica perciò astrattamente lecita per quanto potenzialmente intrusiva della sfera personale; tuttavia quando la propria dimensione soggettiva risulti lesa, nel caso concreto, con un' incidenza definibile importante, sia riscontrabile cioè una certa gradazione dell'offesa – restando al caso esemplificativo, ad esempio, per l'eccessiva intrusività della raccolta dei dati [15] o per l'invasività intollerabile dei banner pubblicitari, o ancora per l'implementazione di meccanismi di *pricing* che sfruttano le specifiche debolezze dell'user per proporgli prezzi d'acquisto elevati e fuori standard – è certamente plausibile pensare che tale pratica incida significativamente e in modo analogo sull'interessato rendendosi opportuna l'applicazione della speciale disciplina di cui al-

[12] Sugli obiettivi economici collegati all'integrazione tecnologica nonché i benefici per il mercato digitale attesi quale conseguenza della maggiore 'fiducia' degli stakeholders nei sistemi di AI se opportunamente regolati in modo da garantire trasparenza, protezione dei dati e della persona umana si vadano COM (2018) 237 final, "L'intelligenza artificiale per l'Europa", pp. 9, 15-16; nonché COM (2019) 168 final "Building Trust in Human-Centric Artificial Intelligence".

[13] Come si vedrà *infra*, infatti, l'utilizzo di trattamenti automatizzati che non rientri nell'ambito dell'art. 22 è comunque soggetto alla disciplina 'comune' sulla protezione dei dati sotto il GDPR.

[14] È però previsto, proprio nel GDPR, il diritto di opporsi alla profilazione per fini di marketing. Si veda *infra*.

[15] Si pensi ai casi di tracking dell'utente attraverso più siti web, magari anche attraverso più devices, per ricavarne preferenze e interessi.

l'art. 22 GDPR (che, come si vedrà, richiede necessariamente, tra le altre cose, ad esempio, il consenso informato dell'interessato: v. *infra*). Ciò in ragione non della violazione di un preciso diritto dell'interessato, ma per via dell'esistenza, comunque, nel caso in questione, di una sua legittima pretesa (ricavabile dal complesso dell'ordinamento) a non essere vittima di pratiche commerciali scorrette o essere manipolato nel formarsi di una sua adesione alla volontà di acquistare un determinato bene [16]; nel caso del *pricing*, anche una sua aspettativa a non essere oggetto di pratiche potenzialmente lesive di *price-discrimination* [17]. Volendo fare un altro esempio, il generale principio di correttezza e non discriminazione, ancora, è alla base della legittima pretesa degli interessati a non vedersi rifiutata con processi automatizzati una domanda di credito online: quest'ultima è un'altra tipica ipotesi di ADM rilevante per l'art. 22, per di più autorevolmente citata esemplificativamente dallo stesso Considerando 71 del Regolamento.

4. Una disciplina 'comune' dei trattamenti automatizzati

Pur interpretando in senso ampio la fattispecie di cui all'art. 22 GDPR, ovviamente non tutti i trattamenti di dati che siano condotti con sistemi informatici o di Intelligenza Artificiale finiscono con l'esservi riconducibili; quantomeno quei trattamenti (marginali) che prevedono nel processo decisionale un significativo intervento dell'uomo (accanto a sistemi di raccolta, analisi e conservazione automatizzata dei dati) rifuggono l'applicazione della rigorosa disciplina che si sta esaminando.

Mentre i trattamenti decisionali automatizzati di cui all'art. 22 sono consentiti solo nelle ipotesi di cui al paragrafo 2, gli altri restano ammissibili, tanto per cominciare, in tutti i casi in cui il trattamento dei dati è considerato lecito a norma dell'art. 6 GDPR (ovvero alle condizioni di cui alle lettere dalla a alla f di detto articolo).

Le speciali salvaguardie che il paragrafo 3 dell'art. 22 impone ai titolari di quei trattamenti non sono qui richieste, in primis l'intervento umano.

Trovano applicazione, tuttavia, nei confronti di ogni trattamento di dati personali condotto con sistemi informatici (ricada o no nell'ambito dell'art. 22) quelli che sono i principi generali del GDPR: può parlarsi a riguardo di una disciplina "comune".

---

[16] Principio che l'ordinamento normalmente prevede, ad esempio, a presidio del consumatore in tutte le ipotesi di acquisto a distanza o fuori dai locali commerciali.

[17] Si pensi a meccanismi di dynamic-pricing che, viziati da *bias*, propongano all'utente prezzi troppo elevati col risultato gravoso di escluderlo dall'accesso equo a determinati beni o servizi.

Tra questi principi generali troviamo, in primis, quello di liceità, correttezza e trasparenza del trattamento (art. 5 (1) (a)); a quest'ultima condizione fanno da pendant il diritto dell'interessato ad essere adeguatamente informato circa il trattamento che lo riguarda e ad essere edotto di tutte le circostanze indicate, a seconda del caso, dagli artt. 13 e 14 (diritto all'informativa) ovvero 15 (diritto di accesso). Seppur non tenuto ai più pregnanti oneri informativi di cui meglio si dirà nel prosieguo e che riguarda il solo caso dei trattamenti *ex* art. 22, il responsabile del trattamento è tenuto in ogni caso a fornire all'interessato un'informativa concisa, trasparente, intellegibile e facilmente accessibile, fornita con linguaggio semplice e chiaro e anche, eventualmente, circostanza importante data la materia di cui ci si occupa, in forma elettronica.

Di specifica rilevanza il principio di correttezza: le tecniche di *Big Data* e profilazione, ad esempio, possono ben facilmente, per bug di programmazione o anche semplicemente perché applicate a data-set incompleti o dati inesatti, condurre a decisioni discriminatorie (si pensi ai rischi connessi a sistemi informatici correntemente utilizzati per la selezione delle risorse umane o per valutare richieste di accesso al credito online, calcolare premi assicurativi in base ai potenziali fattori di rischio, ecc.).

A tale principio si riconnettono quello di accuratezza, esattezza e aggiornamento dei dati (art. 5 (1)(d) GDPR), cui simmetricamente si rifanno i diritti dell'interessato alla rettifica (art. 16), alla cancellazione dei dati (art. 17) e alla limitazione del trattamento (art. 18). L'obbligo per i titolari del trattamento di adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (art. 5 (1)(d) GDPR) e gli accennati diritti di 'autotutela' dell'interessato, che ne garantiscono il controllo sull'accuratezza dei dati coinvolti, nel trattamento assumono notevole importanza nell'ambito dei trattamenti automatizzati e ciò per gli enormi rischi che trattamenti di *data-analysis* possano essere viziati da *bias* e condurre a risultati di rilevante impatto per i soggetti coinvolti [18]. Tali rischi sono ancora maggiori quando ci si trovi davanti a sistemi informatici deduttivi come quelli di *Big Data analytics* o *profiling*, capaci di estrapolare, analizzandoli e mettendoli in correlazione statistica, dati da dati, ampliando esponenzialmente i rischi di scarsa accuratezza del data-set, alla cui qualità e precisione è, ovviamente, inversamente proporzionale il rischio di *machine bias (o algorithmic bias)* ovvero di deduzioni errate da parte di AI *systems* dotati di autonomia decisionale [19].

---

[18] Per approfondire, cfr. G. D'Acquisto, *Qualità dei dati e intelligenza artificiale: intelligenza dai dati e intelligenza dei dati*, in F. Pizzetti (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

[19] Cfr G. D'Acquisto, *op. cit.*

Assumono una peculiare importanza anche i principi, pure questi di generale applicazione, di limitazione delle finalità di trattamento, minimizzazione dei dati e limitazione della loro conservazione (rispettivamente *ex* art. 5(1)(b)(c)(e)GDPR). La normale attitudine dei sistemi appena enunciati a processare enormi quantità di dati, spesso anche originariamente raccolti per scopi diversi da quelli per cui sono trattati [20] rende di assoluta importanza l'obbligo del titolare del trattamento di raccogliere i dati per finalità determinate ed esplicite, limitando il trattamento a quei dati che siano pertinenti e assolutamente necessari rispetto alle finalità per cui sono trattati; come pure, altrettanto rilevante, è l'imposta necessità di conservarli, con mezzi adeguati e sicuri, per un arco di tempo non superiore al conseguimento delle finalità per cui sono trattati, dovendo pure essere esplicitata in modo chiaro l'eventualità di una loro possibile trasmissione a terzi.

Di particolare interesse, parlando di trattamenti condotti attraverso applicazioni di IA, è anche il diritto di opposizione (art. 21 GDPR), soprattutto per la previsione di cui al paragrafo 2 per la quale in caso di dati trattati per finalità di marketing diretto (una delle applicazioni più comuni del profiling) l'opposizione dell'interessato determina l'immediata e definitiva cessazione del trattamento non essendo neppure ammesso, unico caso, il titolare a provare l'eventuale esistenza di ragioni che giustifichino la prevalenza del suo legittimo interesse a proseguire il trattamento [21].

5. Il diritto alla 'intelligibilità' dell'algoritmo: un'interpretazione sistematica e coerente del GDPR

Se quella appena analizzata è la disciplina applicabile ad ogni forma di trattamento dei dati condotta con tecniche automatizzate, è solo ai trattamenti decisionali automatizzati (o ADM) rilevanti ai sensi dell'art. 22 GDPR che si applica invece quella specifica e più rigorosa disciplina sulla trasparenza dell'algoritmo contenuta negli artt. 13 (2)(f),14 (2)(g) e 15 (1)(h) del Regolamento.

Le disposizioni citate, con formulazione identica, prevedono – nel caso degli artt. 13 e 14 nell'ambito dell'informativa, nel caso dell'art. 15 quale contenuto del diritto di accesso – che "l'interessato ha il diritto di essere informato circa l'esistenza di un processo decisionale automatizzato, compresa la profilazione, di cui all'art. 22, paragrafi 1 e 4, e, almeno in tali casi, [a ricevere, ndr] informa-

[20] Si pensi alla profilazione operata a fini di targeted marketing sulla base di dati personali variamente raccolti in merito ai gusti e alle abitudini di un utente sulla rete.

[21] La norma è una novità introdotta col GDPR; lascia trapelare un giudizio di notevole pericolosità da parte del legislatore europeo nei confronti di questa pratica commerciale cui contrappone quale rimedio una forma di tutela assoluta della persona.

zioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato".

Sebbene non poche delle interpretazioni della disposizione citata emerse in dottrina, improntate a forte cautela, ritengono di limitare la portata dell'onere in questione per il titolare del trattamento ad una semplice informativa all'interessato circa l'esistenza di un trattamento decisionale automatizzato [22] idoneo a produrre effetti nei suoi confronti o comunque ad incidere significativamente sulla sua sfera giuridica, è di tutta evidenza come invece il diritto in questione non possa che riferirsi ad un *quid pluris*, il contenuto di detta informativa non sarebbe altrimenti in nulla diverso da quello già comunque dovuto per ogni altro trattamento del dato rendendosi del tutto superflua la specificazione invece espressamente voluta dal legislatore europeo.

Vieppiù, la disposizione in esame esplicitamente aggiunge alla mera notifica di 'esistenza' del processo automatizzato il dovere del titolare del trattamento di fornire *anche* informazioni *aggiuntive* (significativo proprio l'uso della congiunzione *e,* proprio a segnare qualcosa di diverso e *in più*) "almeno in tali casi" – ovvero i trattamenti decisionali di cui all'art. 22, altra prova di una ultroneità del requisito informativo richiesto giustificato proprio dalla particolarità della fattispecie – che siano "significative" sulla "logica" utilizzata dall'algoritmo applicato al trattamento, nonché "l'importanza e le conseguenze previste di tale trattamento per l'interessato". È dunque fuori di dubbio che si tratti di un dovere d'informazione certamente più pregnante di quello normalmente previsto per gli altri trattamenti di dati personali.

Quanto al contenuto, invece, di questo 'diritto conoscitivo' dell'interessato occorre, a parere di chi scrive, operare una distinzione tra l'informazione dovuta ai sensi degli artt. 13 (2)(f) e 14 (2)(g) e quella dovuta quale conseguenza dell'esercizio del diritto di accesso dell'interessato ai sensi dell'art. 15 (1)(h) GDPR.

A dispetto di una formulazione pressoché identica delle disposizioni, infatti – come fatto notare in modo efficacemente argomentato da certa dottrina [23] – mentre nell'ambito dell'informativa le informazioni dovute non possono che riferirsi alla generale funzionalità dell'algoritmo e al tipo di decisioni normalmente attese dal suo funzionamento con valutazione astratta ed *ex ante*, nel caso del diritto d'accesso è più opportuno interpretare la norma traendone un dovere di informazione del titolare del trattamento più pregnante e dettagliato e che attenga alla specifica decisione eventualmente già adottata dal sistema nei confronti

[22] S. Watcher, B. Mittlestadt, L. Floridi, *Why a right to explanation of automated decision-making does not exist in the GDPR*, in *International Data Privacy Law*, vol. 7, 2017, p. 76 ss.

[23] G. Malgieri *et al.*, *op. cit.*

dell'interessato e i passaggi inferenziali che hanno portato la macchina a quel dato output.

La necessità di un'interpretazione tal fatta è la naturale conseguenza di un'interpretazione sistematica e coerente del paragrafo 1, lett. h) dell'art. 15 del Regolamento. Come già visto, infatti, l'art. 22 GDPR, al paragrafo 3, prevede espressamente il diritto dell'interessato destinatario di una misura di ADM a mettere in discussione la decisione automatizzata attraverso la possibilità di ottenere l'intervento umano e cioè di relazionarsi in modo 'dialettico' col titolare del trattamento esprimendo la propria opinione, chiedendo di procedere ad una verifica della decisione e potendo anche, successivamente, contestarne gli assunti. Si tratta di un diritto, a ben vedere, che, salvo a volerne frustrare il contenuto sostanziale, sottende necessariamente, da parte dell'interessato (e quindi richiede al titolare del trattamento) un'informazione specifica sul funzionamento dell'algoritmo, non astratta e pronostica ma concreta ed *ex post,* calata nell'applicazione specifica che lo riguarda; solo in tal modo infatti l'interessato sarebbe messo in condizione di esercitare appieno il suo diritto oppositivo, disponendo degli strumenti idonei a muovere una contestazione specifica e motivata. Non è un caso infatti - a parere di chi scrive – che il Considerando 71 al Regolamento espressamente metta in relazione questi due diritti dell'interessato elencando, tra le garanzie opportune che si dovrebbero accompagnare a trattamenti decisionali automatizzati, "la specifica informazione dell'interessato e il diritto di ottenere l'intervento umano [...]", parlando, per di più, significativamente, proprio di "un'informazione *specifica*" [24].

Nello stesso senso si è espresso lo High Level Expert Group on Artificial Intelligence (AI HLEG), gruppo di esperti istituito dalla Commissione europea con le Comunicazioni del 25 aprile e del 7 dicembre 2018 con lo specifico compito di individuare, nel quadro dei valori e dei principi giuridici dell'UE, precisi orientamenti etici atti a governare uno sviluppo socialmente sostenibile dell'Intelligenza Artificiale. Nel documento pubblicato il 8 aprile 2019, e significativamente intitolato "Orientamenti Etici per un'IA affidabile", il consesso, dopo aver individuato una serie di principi fondamentali, tra cui l'equità, cui il nuovo quadro tecnologico dovrebbe informarsi per essere "*trustworthy*", cioè per far sì che gli esseri umani e le comunità possano riporvi fiducia ed affidarsi all'uso delle nuove applicazioni tecnologiche dando così slancio al mercato digitale con tutti i benefici espansivi che comporta, significativamente afferma: "*La dimen-*

[24] Interpretazione diversa, va segnalato, propone nelle *Linee guida* il WP29 per cui l'onore informativo *ex* art. 15 (1)(h) GDPR dovrebbe consistere in una "*information about the envisaged consequences of the processing rather than an explanation of a particular decision".* Cfr. Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, n. 251* del 3 ottobre 2017, p. 27.

sione procedurale dell'equità implica la capacità di impugnare le decisioni elaborate dai sistemi di AI […] *e la possibilità di presentare un ricorso efficace contro di esse. A tal fine* […] *i processi decisionali devono essere spiegabili*". Ivi, ancora, più specificatamente sull'esplicabilità, si aggiunge: "*Tale principio implica che i processi devono essere trasparenti, le capacità e lo scopo dei sistemi di AI devono essere comunicati apertamente e le decisioni, per quanto possibile, devono poter essere spiegate a coloro che ne sono direttamente o indirettamente interessati. Senza tali informazioni una decisione non può essere debitamente impugnata*" [25].

Ultimo punto che resta da affrontare è cosa si intenda per "informazioni significative sulla logica utilizzata, l'importanza e le conseguenze previste di tale trattamento per l'interessato". È opinione di chi scrive che, alla luce di un'interpretazione che, anche in questo caso, guardi al contesto delle disposizioni regolamentari – in particolare ai requisiti di chiarezza, intelligibilità, accessibilità, semplicità di linguaggio che presidiano all'informazione cui ha diritto in via generale l'interessato soggetto a un trattamento dei propri dati personali *ex* art. 12 (1) GDPR – deve escludersi che il legislatore europeo voglia riferirsi ad un obbligo di mera 'trasparenza' dell'algoritmo, soprattutto se inteso nella sua veste matematica come cioè architettura di sistema, dovendosi piuttosto ritenere che quello che qui interessa, e compete al titolare del trattamento esplicare – magari in aggiunta alla funzione matematica che sostanzia l'algoritmo in questione – è la sua concreta implementazione: il contesto in cui è applicato, gli scopi perseguiti, le tecniche applicate e magari anche degli esempi circa il suo concreto funzionamento. Solo allegando tali circostanze all'informativa dovrebbe potersi ritenere assolto quel dovere "esplicativo" che il legislatore sembrerebbe richiedere.

Alla luce di ciò, ecco spiegato perché [26] si è voluto connotare il diritto dell'interessato di cui agli artt. 13 (2)(f),14 (2)(g) e 15 (1)(h) del Regolamento come un diritto alla 'intellegibilità' dell'algoritmo, volendosi in qualche modo, con tale espressione, tradurre quella di '*legibility*' usata per la prima volta da Richard Mortier [27] proprio per riferirsi ad una *disclosure* dell'algoritmo che riassumesse la trasparenza del programma unitamente alla comprensibilità del suo funzionamento da parte degli individui ad esso soggetti o potenzialmente interessati dal suo funzionamento.

---

[25] *Ethics guidelines for trustworthy AI* (AI HLEG), 2019, paragrafi 52 e 53. Available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[26] Anche sulla scorta e l'intuizione di G. Malgieri *et al.*, *op. cit.*

[27] R. Mortier *et al.*, *Human data interaction: The human face of the data-driven society*, in *MIT Technology Review*, 2014.

6. L'Accountability, l'obbligo di DPIA e il ruolo della privacy by design e by default nel futuro di una data-driven society

Un ultimo aspetto su cui vale la pena soffermarsi, fisiologicamente in conclusione di questa breve trattazione, è l'accountability, ovvero il principio di responsabilizzazione del titolare del trattamento per cui quest'ultimo, ai sensi dell'art. 5 (2) GDPR, è chiamato a comprovare il rispetto delle norme sulla protezione dei dati.

È in questa sede infatti che il titolare del trattamento, stando all'art. 24 del Regolamento - tenuto conto della natura, del contesto e delle finalità del trattamento, valutati pure tutti i rischi ad esso contestuali per i diritti e le libertà individuali – è tenuto a dimostrare che il trattamento è effettuato in modo conforme al GDPR e cioè che sono rispettati tutti i principi e le condizioni, anche specifiche, che informano il trattamento dei dati e che tutti i diritti stabiliti dalla legge a presidio degli interessati, attuali o potenziali, sono adeguatamente garantiti. Il titolare del trattamento – prima di procedere allo stesso come pure, periodicamente, nel corso di questo – deve individuare il tipo di trattamento che si appresta ad eseguire, i dati e i soggetti coinvolti, valutarne la probabilità e la gravità dei rischi e dar prova di aver diligentemente ottemperato a tutti gli obblighi di protezione del caso.

È in punto di accountability, ad esempio, che, ove il trattamento importi processi automatizzati, il titolare deve provare che questo non ricada nell'ambito dell'art. 22 ove non voglia o non possa rispettarne le condizioni; viceversa, laddove ritenga si tratti di ADM basato unicamente su trattamenti automatizzati, è sempre in questo contesto che deve dimostrare di aver adempiuto a tutti gli oneri informativi richiesti dal Regolamento e adottato misure di salvaguardia adeguate.

Si tenga anche presente che, ai sensi dell'articolo 35 del GDPR, "quando il trattamento prevede l'uso [...] di nuove tecnologie" e "può presentare un rischio elevato per i diritti e le libertà della persona fisica" il titolare del trattamento è pure obbligato a svolgere (consultandosi col DPO, ove nominato) una specifica valutazione di impatto del trattamento sulla protezione dei dati (o DPIA); essa è peraltro in ogni caso obbligatoria (ai sensi del paragrafo 3 dell'art. 35) quando si pongano in essere "trattamenti che comportano una valutazione globale e sistematica degli aspetti relativi alle persone fisiche, basate su un trattamento automatizzato, compresa la profilazione, sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche" [28].

[28] Si evidenzia che la disposizione citata discorre di decisioni "basate su" trattamenti automa-

Ai fini di questa valutazione un *auditing* dell'algoritmo, una cioè chiara esplicazione del suo funzionamento risulta non solo strumentale a quell'onere suddetto di 'intellegibilità' del processo automatizzato – prevista a beneficio dei soggetti interessati - ma è pure essenziale al titolare del trattamento proprio per assolvere al suo impegno di accountability: solo esplicando nel dettaglio il funzionamento dei processi decisionali automatizzati che governano il trattamento questi potrà comprovare il rispetto del GDPR [29], ben difficilmente potendosi immaginare che un black-box algorithm – perché tenuto volontariamente segreto o perché magari dal funzionamento addirittura non prevedibile nei suoi concreti esiti neppure da chi lo abbia predisposto o implementato – sia idoneo ad assicurare, tanto per fare un esempio, il rispetto della limitazione del trattamento o la minimizzazione della raccolta dei dati.

È importante ricordare, inoltre, che il titolare del trattamento non può limitarsi ad assolvere gli oneri cd. informativi, o garantire i diritti dell'interessato che sia soggetto al trattamento automatizzato; a norma dell'art. 24 del Regolamento esso è tenuto pure ad 'attivarsi' mettendo in atto misure tecniche e organizzative adeguate al caso concreto per garantire la *compliance* al GDPR, e questo è un obbligo che richiede non solo una *disclosure* dell'algoritmo ma anche, a monte, una corretta predisposizione o selezione degli strumenti di Intelligenza artificiale più adatti ad assicurare una corretta protezione dei dati personali e dei diritti e delle libertà dei soggetti coinvolti. Le metodologie cui il titolare del trattamento ricorre a tal fine sono quelle di cui all'art. 25 del Regolamento della privacy by design e by default, ovvero, con l'improvvida traduzione italiana, della protezione dei dati fin dalla progettazione e per impostazione predefinita.

La pianificazione delle misure tecniche da applicarsi ad uno specifico trattamento e alle sue particolari criticità in modo da minimizzarne i rischi (privacy by design) e ancor di più la corretta ideazione e definizione, a monte, degli strumenti e delle applicazioni informatiche da adoprarsi per il trattamento in modo da garantire che, per impostazione predefinita, sia *privacy-compliant* (privacy by default), acquistano quindi, nell'humus di questa sempre più *data-driven society* un ruolo di primissimo piano rappresentando lo strumento principe in grado di raccogliere la sfida del futuro della protezione dei dati come pure del mercato digitale [30]: chiunque voglia servirsi di applicazioni di AI, Big Data

---

tizzati e non invece di decisioni "basate unicamente su" trattamenti automatizzati, con la conseguenza che la fattispecie copre, ma è più ampia di quella *ex* art. 22 (1) GDPR. Cfr. Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, n. 251* del 3 ottobre 2017, p. 29.

[29] Per approfondire v. G. Malgieri *et al.*, *op. cit.*

[30] Su come il modello di accountability del GDPR e gli strumenti di privacy by design possano assurgere a modello efficace per la gestione computazionale ed automatizzata dei vari profili di

Analytics, IoT ecc. o anche solo offrire tali servizi sul mercato dovrà fare i conti con l'accountability del GDPR – direttamente i titolari del trattamento, indirettamente gli informatici, sviluppatori e produttori di questi sistemi – tutti chiamati a sforzarsi di costruire sistemi non solo tecnologicamente evolutivi ma sempre più *privacy-compliant*, progettati per assolvere efficacemente a determinate finalità pratiche ma pur sempre in modo da garantire il rispetto non solo delle regole sulla protezione dei dati a più in generale dei diritti e delle libertà della persona che ne possano risultare minacciati [31].

7. Impressioni conclusive

Il GDPR, dunque, concludendo, non vuole porre un limite alla tecnologia, ma piuttosto indicare una direzione o, meglio ancora, un binario entro il quale questa è libera di correre, sempre più veloce, senza deragliare nella violazione dei diritti umani o incrociare la corsa con le libertà fondamentali dell'individuo, ma piuttosto mettendo al servizio di queste la sua velocità in una comune corsa al futuro (e ci si augura, per il meglio). E mentre si è già in arrivo alla prossima stazione, e la fantasia diventa ingegneria, già si immaginano (e costruiscono) i primi sistemi di machine learning che, interiorizzati principi etico-giuridici, siano in grado di assumere in autonomia tutte le scelte procedimentali più opportune per adeguare, dinamicamente ed in modo automatico, il trattamento alle via via emergenti necessità di tutela degli interessati. Funzionerà? A giudici robot l'ardua sentenza.

responsabilità civile dei robot e delle AI technologies si legga G. Comandé, *Responsabilità ed accountability nell'era dell'Intelligenza Artificiale,* in Di Ciommo, Troiano (a cura di), *Giurisprudenza e Autorità Indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi*, Piacenza, 2018, p. 1001 ss.; su come principi etico-giuridici possano, e debbano, essere implementati nella progettazione dei sistemi di AI, una sorta di *Ethics by design*, cfr. *Ethics guidelines for trustworthy AI* (AI HLEG), 2019, paragrafo 98. Available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[31] Per approfondire, F. Pizzetti (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Torino, 2018.