



Alessandro Moretti

**ALGORITMI E DIRITTI
FONDAMENTALI DELLA
PERSONA. IL CONTRIBUTO DEL
REGOLAMENTO (UE) 2016/679**

Estratto



GIUFFRÈ FRANCIS LEFEBVRE

ALESSANDRO MORETTI

ALGORITMI E DIRITTI FONDAMENTALI DELLA PERSONA. IL CONTRIBUTO DEL REGOLAMENTO (UE) 2016/679

SOMMARIO: 1. Cenni introduttivi: dati, algoritmi e Big Data Analytics. — 2. L'impatto sui diritti e sulle libertà dell'individuo. — 3. Il contributo del Regolamento (UE) 2016/679. — 3.1. Le garanzie conoscitive. — 3.2. Il divieto di processi decisionali automatizzati. — 3.3. *Right to explanation*, DPIA e categorie particolari di dati. — 4. Riflessioni conclusive.

1. CENNI INTRODUTTIVI: DATI, ALGORITMI E BIG DATA ANALYTICS.

La rivoluzione tecnologica ha inciso profondamente sulla nostra quotidianità, influenzando con forza sulle abitudini, sui comportamenti e sui processi decisionali tanto dei singoli quanto delle imprese. Il mutato contesto tecnologico consente la datizzazione¹ di qualsiasi fenomeno ed accresce, contestualmente, la capacità di produrre, archiviare e conservare enormi moli di dati, realizzando i presupposti per l'affermazione del nuovo paradigma dei *Big Data*².

L'effettivo valore dei dati, tuttavia, non è rappresentato dal loro mero possesso o dalla quantità, ma è connesso alla capacità

* Il presente lavoro è stato preventivamente sottoposto a referaggio secondo le prassi correnti nella comunità dei giuristi.

¹ Con il termine "datizzazione" si indica la tendenza a convertire un fenomeno in forma quantitativa, in dato, in modo da poterlo raccogliere, tabulare ed analizzare. Così, V. MAYER-SCHÖNBERGER, K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, Garzanti, 2013, 109 e 130. Al riguardo in L. TREMOLADA, *Informazioni emergenti*, in *La miniera dei big data*, Il Sole 24 ORE, Nòva edu - Lezioni di futuro, Dicembre 2015, II, 6 ss., si evidenzia che anche gli esseri umani sono da intendersi come fenomeni misurabili e quantificabili.

² Il concetto di *Big Data* è stato tradizionalmente descritto attraverso il modello delle "3V" (volume, varietà e velocità) da D. LANEY, *3-D data management: Controlling data volume, velocity and variety*, Application Delivery Strategies by META Group Inc., 6 Febbraio 2001, reperibile in <https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3-D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>. Il tema dei *Big Data* è stato recentemente affrontato in G. D'ACQUISTO, M. NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, Giappichelli, 2017, 5 ss. Gli Autori illustrano il passaggio da un approccio *Small Data* ad una prospettiva *Big Data* attraverso una riflessione incentrata « sulla differenza che esiste tra cercare e tro-

di elaborazione dei dati in modo tale da valorizzarne il potere informativo e da generare nuova conoscenza. La modalità attraverso cui i dati vengono trattati risulta determinante per estrarre valore e per evitare che gli stessi si rivelino improduttivi, se non addirittura fuorvianti, in ragione delle risultanze di un'erronea attività di analisi³. Il mutamento che si sta attraversando, dunque, non è solo quantitativo, legato al volume e alla varietà dei dati in nostro possesso, ma è soprattutto qualitativo, in ragione delle modalità innovative attraverso cui elaborare dati e condurre processi decisionali⁴.

È lo sviluppo di *Big Data Analytics*⁵, ossia di algoritmi e modelli di analisi, che assume un ruolo centrale nelle dinamiche economiche, politiche e sociali, dando la possibilità di svolgere indagini su larga scala e di adottare, allo stesso tempo, strategie altamente personalizzate⁶. L'utilizzo di *Big Data Analytics* rappresenta per i soggetti pubblici l'opportunità di identificare con precisione le esigenze dei cittadini e di realizzare, conseguentemente, l'erogazione di servizi che assicurino un maggiore benessere per la collettività. Allo stesso modo, i *Big Data Analytics* costituiscono una preziosa occasione di crescita per le imprese, in grado di aumentare l'efficienza organizzativa interna e di strutturare al meglio l'offerta dei propri servizi⁷.

I vantaggi connessi all'analisi dei dati sono molteplici ed alquanto seducenti per i soggetti pubblici e per le imprese che

vare, sul "costo" che sussiste nel passaggio tra l'una e l'altra attività e su chi lo sostiene ».

³ Sulla centralità dell'analisi dei dati, oltre al loro mero possesso, A. MANTELERO, *The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer Law & Security Review*, December 2014, 30, VI, 650.

⁴ In tal senso A. SORO, *Liberi e connessi*, Torino, Codice Edizioni, 2016, 20.

⁵ Si veda A. PIVA, I. GUIDANI, *Il contesto di riferimento*, in *Big Data Analytics: leve di progettazione, sfide e opportunità, ambiti di applicazione*, Il Sole 24 ore, Settembre 2017, 14 ss., i quali, parallelamente al modello delle "3V", evidenziano l'importanza del valore che può essere estratto attraverso i modelli di analisi dei dati, ossia i *Big Data Analytics*. Gli Autori identificano quattro principali categorie di *Big Data Analytics*: *Descriptive Analytics*, *Predictive Analytics*, *Prescriptive Analytics* e *Automated Analytics*.

⁶ In tal senso A. MANTELERO, *I Big Data nel quadro della disciplina europea della tutela dei dati personali*, in *Il Corriere giuridico - Speciali Digitali 2018*, IP-SOA, 2018, 46, indica che i *Big Data*

Analytics consentono il superamento, o comunque l'integrazione, del tradizionale approccio statistico-campionario incentrato sull'estrazione e sull'analisi di campioni statistici rappresentativi.

⁷ Si veda V. MORABITO, *Big Data and Analytics. Strategic and Organizational Impacts*, Springer, 2015, 23 ss. indica possibili vantaggi dell'utilizzo di *Big Data Analytics* per i soggetti pubblici tra i quali, a titolo esemplificativo, l'attività di *crowdreporting* attraverso cui incentivare la partecipazione e la cooperazione dei cittadini. Ulteriori esempi vengono illustrati nell'ambito della sanità, dell'istruzione e del trasporto dall'Autorità inglese Garante per la protezione dei dati personali in INFORMATION COMMISSIONER'S OFFICE, *Big data, artificial intelligence, machine learning and data protection*, 2017, 15 ss. Cfr. I. GUIDANI, *I progetti di Big Data Analytics*, in *Big Data Analytics: leve di progettazione, sfide e opportunità, ambiti di applicazione*, Il Sole 24 ore, Settembre 2017, 46 ss., suggerisce talune modalità di analisi di dati particolarmente vantaggiose per le imprese, tra i quali, la manutenzione predittiva, la mappatura dei comportamenti, l'ottimizzazione del prezzo e delle scorte, la previsione della domanda.

aspirano alla massimizzazione del profitto e ad acquisire un vantaggio competitivo sul mercato, ma anche per i singoli individui che posso usufruire di offerte su misura e di servizi personalizzati. Non bisogna, tuttavia, rimanere abbagliati dalle opportunità di crescita e dai vantaggi che il nuovo mondo digitale ha messo a nostra disposizione. All'utilizzo diffuso di algoritmi per l'elaborazione dei dati e per l'implementazione di processi decisionali automatizzati si accompagnano profondi rischi per i cittadini, i quali, sempre più, rischiano di essere condizionati, anche inconsapevolmente, nei propri comportamenti e di essere vittime di trattamenti profondamente discriminatori.

2. L'IMPATTO SUI DIRITTI E SULLE LIBERTÀ DELL'INDIVIDUO.

L'utilizzo di sofisticati sistemi di analisi ha fatto emergere un elevato rischio per gli individui che non interessa solamente una possibile lesione del diritto alla protezione dei dati personali, ma che riguarda, in modo più ampio, i diritti e le libertà fondamentali della persona⁸. Particolari criticità emergono dalla diffusione di complessi algoritmi che, elaborando grandi moli di dati, vengono impiegati per indagare la personalità dell'individuo e conoscerne gli aspetti più intimi, sino al punto di essere utilizzati per prendere decisioni suscettibili di avere un forte impatto sulla persona.

Dal momento che il concetto e l'utilizzo degli algoritmi è inscindibile da quello di dato — gli algoritmi vengono sviluppati ed “allenati” attraverso grandi moli di dati — risulta di immediata evidenza che la qualità e la veridicità dei dati stessi sia determinante affinché il procedimento matematico possa condurre ad un risultato affidabile.

Un processo nel quale vengano elaborati dati errati o non aggiornati, non effettivamente rappresentativi della realtà, può avere infatti conseguenze negative sulla sua sfera giuridica e personale dell'individuo⁹. Sarebbe profondamente ingiusto essere esclusi da un concorso per agenti di polizia solo perché un algoritmo ha confuso il nostro nominativo con quello di un

⁸ In questo senso J. PODESTA, *Big data: Seizing opportunities, preserving values*, White House, Executive Office of the President, United States, 2014, 51. In N. M. RICHARDS, J. H. KING, *Three Paradoxes of Big Data*, in *Stanford Law Review Online*, September 2013, 66, 44 ss., si rileva che i rischi per i diritti e le libertà della persona siano ancora più intensi dal momento che la capacità di eseguire complesse attività di elaborazione dei dati è limitata a pochi soggetti, pubblici o privati, e non anche alle persone comuni.

⁹ Al riguardo si veda C. O'NEIL, *Armi*

di distruzione matematica. Come i Big Data aumentano la disuguaglianza e minacciano la democrazia, Milano, Bompiani, 2017, 219 ss., la quale sostiene che dall'elaborazione di dossier inesatti attraverso procedimenti automatizzati privi di una supervisione umana deriverà probabilmente un alto tasso di decisioni errate. Si riporta come esempio l'attestazione di affidabilità creditizia. Sul l'argomento ARTICLE 29 WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 3 October 2017 - revised on 6 February 2018, 12.

pregiudicato, e sarebbe altrettanto iniquo non ricevere un prestito poiché si è scambiati per un omonimo con una scarsa affidabilità creditizia. Il rischio che si corre è di generare un meccanismo di *garbage in, garbage out* secondo cui l'elaborazione di dati qualitativamente scadenti determina in modo inevitabile risultati fuorvianti, informazioni personali non corrispondenti alla realtà e, talvolta, vere e proprie sovrapposizioni di identità.

Se la carenza qualitativa dei dati può determinare un meccanismo di *garbage in, garbage out* che impatta negativamente sull'individuo, rilevanti conseguenze discriminatorie possono derivare ancor prima dallo schema su cui è messo a punto l'algoritmo e dall'obiettivo che si vuole perseguire attraverso il suo utilizzo ¹⁰.

È opportuno rilevare che gli algoritmi sono da intendersi quali processi neutri, di per sé né giusti né discriminatori, ed è proprio simile carattere neutrale che presta il fianco alla possibilità che il processo matematico rifletta precise ideologie e ripeta pratiche e modelli preesistenti ¹¹. In questo senso, risulta determinante il momento di messa a punto dell'algoritmo e l'attività dei soggetti a ciò preposti, i *Data Scientists*, poiché è in questa fase che specifiche convinzioni radicate nella realtà possono venire cristallizzate all'interno del processo matematico.

Ciò può essere frutto di una precisa scelta da parte dello sviluppatore dell'algoritmo al fine di mascherare propri pregiudizi dietro ad un'apparente oggettività matematica. Il più delle volte, però, gli algoritmi possono risultare dannosi nonostante siano stati predisposti con le migliori intenzioni, soprattutto laddove il modello matematico, essendo sviluppato da soggetti operanti nel mercato, risponde principalmente ad esigenze di massimizzazione del profitto senza dedicare particolare attenzione al profilo etico ed equitativo. La cristallizzazione di convinzioni preesistenti, infatti, non rispecchia necessariamente una espressa volontà dei *Data Scientists*, ma può derivare in modo inconsapevole dalla scelta delle categorie di dati da analizzare, dall'obiettivo che si vuole perseguire e dai pregiudizi radicati nella società. D'altro canto i dati rappresentano fenomeni del passato, con la conseguenza che, attraverso la loro elaborazione, l'algoritmo proietta nel futuro retaggi passati favorendo la persistenza di ideologie e pregiudizi ¹².

¹⁰ Cfr. V. MAYER-SCHÖNBERGER, K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, cit., 224.

¹¹ In questo senso C. O'NEIL, *Armi di distruzione matematica. Come i Big Data aumentano la disuguaglianza e minacciano la democrazia*, cit., 33, secondo cui gli al-

goritmi « nonostante la loro reputazione di imparzialità, sono il riflesso di obiettivi e ideologie ».

¹² Si veda S. BAROCAS, A. D. SELBST, *Big data's disparate impact*, in *California Law Review*, 2016, 104, 680 ss. e 688 ss., i quali mostrano quanto sia rilevante la scelta dei dati attraverso cui "allenare" l'algo-

L'assimilazione di logiche discriminatorie all'interno di modelli matematici risulta particolarmente odiosa dal momento che gli algoritmi corrono il rischio di instaurare cicli di *feedback* negativo e soffrono, il più delle volte, di una forte carenza di trasparenza.

Ogni modello matematico necessita di periodici riscontri attraverso cui valutare se il processo delineato richieda interventi migliorativi o possa essere ritenuto affidabile. L'assenza di un qualsivoglia coinvolgimento umano nel corso del procedimento alimenta il pericolo che l'algoritmo, autoalimentandosi attraverso i suoi stessi risultati, giustifichi l'apparente correttezza del modello adottato. L'algoritmo andrebbe così a produrre un ciclo di *feedback* negativo che approfitta delle risultanze dell'analisi svolta per legittimare e perpetuare il proprio schema con effetti estremamente distorsivi.

Pensiamo all'utilizzo da parte delle forze di polizia di un algoritmo predittivo per individuare quali aree siano maggiormente a rischio di reati gravi, affinché le forze di polizia possano allocare efficientemente le risorse a loro disposizione. Da un lato escludiamo che l'algoritmo tenga in considerazione categorie di dati che potrebbero cristallizzare pregiudizi preesistenti all'interno del processo matematico. Dall'altro lato immaginiamo che l'algoritmo, sulla presunta correlazione tra reati minori e reati gravi, vada anche ad elaborare i dati relativi a reati bagatellari per acquisire una maggiore precisione predittiva. Le forze di polizia presidieranno, dunque, quelle zone che l'algoritmo identificherà più a rischio. L'assidua presenza della polizia in dette zone accrescerà esponenzialmente l'indice dei reati bagatellari commessi, dal momento che quest'ultimi sono reati punibili per lo più solo se compiuti sotto gli occhi di un pubblico ufficiale. Inoltre bisogna considerare come sia più facile che un ubriaco torni a compiere atti osceni nello stesso luogo, piuttosto che un ladro torni a rubare nella stessa casa. Il tasso di reati bagatellari aumenterà in modo esponenziale rispetto alla percentuale dei reati gravi, acquisendo di conseguenza un peso maggiore nella determinazione del risultato dell'analisi algoritmica. I risultati prodotti andranno ad innescare un ciclo di *feedback* negativo che, rafforzando il convincimento secondo cui le zone identificate sono effettivamente quelle con il più alto tasso di criminalità, giustificherà ulteriori e più decisi interventi di polizia.

ritmo e l'individuazione delle caratteristiche da tenere in considerazione nel processo matematico, anche attraverso l'utilizzo di dati vicarianti. Si evidenzia inoltre come l'algoritmo possa assorbire nel proprio meccanismo i pregiudizi radicati nella società, determinando trattamenti discriminatori

verso soggetti che già si trovano in una posizione di debolezza. Così L. CARMICHAEL, S. STALLA-BOURDILLON, S. STAAB, *Data mining and automated discrimination: a mixed legal/technical perspective*, in *IEEE Intelligent Systems*, November 2016, 31, VI, 51.

Si è partiti ipotizzando un algoritmo finalizzato alla prevenzione di reati gravi che non facesse propri eventuali pregiudizi radicati nella società. Si è giunti, invece, ad un algoritmo che si concentra quasi esclusivamente su reati di scarsa rilevanza e che giustifica la correttezza del modello adottato attraverso i suoi stessi risultati. Un algoritmo che, pur apparendo coerente e funzionante, da un lato è andato fuori strada deviando dall'obiettivo originario, e che dall'altro lato, in assenza di un controllo umano sul processo matematico, continuerà a trovare applicazione perpetuando l'erroneo convincimento di perseguire efficacemente l'obiettivo iniziale¹³.

La pericolosità di un ciclo di *feedback* negativo è ulteriormente amplificata dall'opacità e dall'aura di mistero che avvolge l'algoritmo. I modelli matematici corrono il rischio di apparire come scatole nere dal contenuto segreto e imperscrutabile, non essendo possibile osservarne il funzionamento e, in ogni caso, risultando arduo comprenderne il meccanismo. I processi decisionali si caratterizzano per non essere visibili dall'esterno, in modo particolare dai soggetti direttamente coinvolti dalla decisione, e talvolta addirittura dall'interno, si pensi ai casi in cui il processo matematico rilevi delle correlazioni e dei *patterns* del tutto inaspettati per i *Data Scientists*. L'opacità degli algoritmi, inoltre, rimane tanto più difficile da dipanare quanto più il diritto d'autore viene richiamato a difesa della segretezza del modello matematico. La proprietà intellettuale viene diffusamente utilizzata come decisa argomentazione contro le istanze volte ad una maggiore trasparenza, soprattutto da parte di quelle società internazionali che fondano la loro stessa linfa vitale nella raccolta massiva e nell'elaborazione dei dati¹⁴.

Simili considerazioni rivelano come gli algoritmi tendano ad essere caratterizzati da una drammatica carenza di trasparenza, particolarmente grave dal momento che quest'ultima assume fondamentale importanza affinché il cittadino possa controllare l'andamento dei processi automatizzati, comprenda le ragioni che hanno condotto ad una determinata decisione e possa individuare

¹³ Si veda C. O'NEIL, *Armi di distruzione matematica. Come i Big Data aumentano la disuguaglianza e minacciano la democrazia*, cit., 11 ss. e 127 ss., in cui si illustrano i cicli di *feedback* negativo che possono derivare, ad esempio, dall'utilizzo di algoritmi per valutare il rendimento degli insegnanti o per la prevenzione dei crimini.

¹⁴ La ricerca di un bilanciamento tra gli interessi connessi alla proprietà intellettuale e la tutela della persona è posta in evidenza da G. MALGIERI, G. COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protec-*

tion Regulation, in *International Data Privacy Law*, November 2017, 7, IV, 262 ss. Al riguardo, in V. MAYER-SCHÖNBERGER, K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, cit., 161 ss., si rileva che gran parte della ricchezza di società come Facebook, Google e Amazon corrisponde agli *asset* intangibili — i dati — e alle modalità con cui questi vengono elaborati. Per simili società svelare l'algoritmo attraverso cui i dati sono processati determinerebbe uno svantaggio competitivo enorme.

in concreto a chi sia ascrivibile la responsabilità della scelta¹⁵. Dall'assenza di trasparenza deriva per il soggetto una sostanziale inappellabilità della decisione, un risultato incontestabile che evidenzia la vulnerabilità dell'interessato incapace di comprendere l'esito del processo matematico e di opporsi e quella che si potrebbe definire una dittatura dell'algoritmo¹⁶.

I rischi connessi alla diffusione di algoritmi e di processi decisionali automatizzati risultano ancor più critici e di complessa risoluzione potendo manifestarsi, paradossalmente, anche laddove non siano presenti dati relativi a specifici gruppi di individui. Trattamenti discriminatori possono derivare non solo da un'estrema inclusione prodotta dai *Big Data* e degli strumenti di *Analytics*, ma anche da una condizione di sostanziale emarginazione. Si fa riferimento a quelle persone che si trovano all'esterno del flusso quotidiano di dati a causa di condizioni geografiche, culturali, di povertà o di incapacità all'utilizzo delle nuove tecnologie.

L'assenza di dati può condurre a decisioni aziendali e offerte di beni e servizi che non tengano in considerazione le esigenze specifiche di tali persone. Conseguenze ancor più drammatiche possono derivare qualora la mancanza di dati determini da parte delle Istituzioni una condizione di sostanziale marginalizzazione nei confronti di singoli cittadini o di specifici gruppi, i quali perderebbero l'opportunità di influire e partecipare alla cosa pubblica¹⁷. Se è essenziale che a ciascuno sia assicurata la possibilità di gestire e proteggere la crescente mole di dati personali che lo riguarda, è parimenti necessario, dunque, salvaguar-

¹⁵ Cfr. N. M. RICHARDS, J. H. KING, *Three Paradoxes of Big Data*, cit., 42 ss., il quale indica che ragioni di ordine legale, tecnico e commerciale rischiano di avvolgere nel segreto i processi di analisi. Così V. MAYER-SCHÖNBERGER, K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, cit., 240 ss. Al riguardo si è pronunciato l'EUROPEAN DATA PROTECTION SUPERVISOR, Opinion 7/2015, *Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability*, 19 November 2015, 10, che ha evidenziato l'importanza di una maggiore trasparenza dei processi decisionali automatizzati al fine di poter osservare all'interno della *black box* dei modelli matematici. Sul tema V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Rivista di diritto dei media*, 2013, II, 5-6, il quale evidenzia l'importanza connessa alla trasparenza degli algoritmi e all'individuazione di parametri pro-

fessionali per la loro elaborazione, rilevando, inoltre, l'opportunità di un'attenta *data accountability* che vigili sui processi decisionali automatizzati.

¹⁶ Si veda S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, Laterza, 2012, 401 ss. L'Autore analizza la criticità di un incondizionato e pervasivo utilizzo degli algoritmi nella società dell'informazione, sostenendo che « quando l'algoritmo diviene il fondamento del potere esercitato da un soggetto (...), e tutto ciò che lo riguarda è avvolto nella massima segretezza, allora siamo davvero di fronte ad una nuova versione degli *arcana imperii* ».

¹⁷ Al riguardo J. LERMAN, *Big Data and Its Exclusions*, in *Stanford Law Review Online*, September 2013, 66, 55 ss., il quale indica l'opportunità di tenere in considerazione un *right to be not forgotten* per quei soggetti che si trovano al di fuori del flusso quotidiano dei dati, affinché di fatto non si realizzi nei loro confronti un procedimento di esclusione.

dare quelle realtà che rimangono fuori dal quotidiano flusso informativo e che, non alimentando modelli matematici attraverso dati propri, corrono il rischio di risultare invisibili agli occhi della società.

Quanto osservato mostra come le criticità che caratterizzano l'utilizzo degli algoritmi rendono necessaria l'elaborazione di nuove modalità che garantiscano i diritti fondamentali della persona all'interno del mondo digitale. Risulta indispensabile un intervento giuridico e culturale che, associando all'utilizzo dei processi matematici non solo il valore dell'efficienza ma anche quello dell'equità, esalti il ruolo ed il valore della persona umana ed escluda una completa abdicazione in favore dell'algoritmo.

3. IL CONTRIBUTO DEL NUOVO REGOLAMENTO (UE) 2016/679.

3.1. *Le garanzie conoscitive.*

La rivoluzione tecnologica e il diffuso utilizzo di algoritmi all'interno dei processi decisionali hanno posto in evidenza l'obsolescenza della normativa europea in materia di protezione dei dati personali, sprovvista di strumenti utili a fronteggiare le sfide del nuovo mondo digitale. Il maturare di una simile consapevolezza ha portato all'adozione del Regolamento (UE) 2016/679, che abroga la Direttiva 95/46/CE, con l'obiettivo di implementare le garanzie poste a tutela dell'autodeterminazione informativa della persona alla luce dell'evoluzione tecnologica. È bene evidenziare che l'importanza del nuovo Regolamento non deve essere circoscritta al solo ambito della protezione dei dati personali. Esso risulta un intervento normativo che, nel mutato contesto tecnologico, pone attenzione agli algoritmi e ai processi decisionali automatizzati, problematizzandosi, in modo più ampio, circa i potenziali rischi per i diritti e le libertà fondamentali della persona ¹⁸.

Ad oggi nelle attività di trattamento dei dati personali possono essere individuate due differenti tipologie di processi decisionali automatizzati: quelli che contemplanò un coinvolgimento umano e quelli che, al contrario, affidano al solo algoritmo l'intero procedimento. Il Regolamento, concentrandosi su tali modalità di elaborazione dei dati, integra la disciplina già contenuta nella Direttiva 95/46/CE con l'intento di arginare il rischio di trattamenti

¹⁸ In questo senso B. W. GOODMAN, *A step towards accountable algorithms?: algorithmic discrimination and the european union general data protection*, 29th Conference on Neural Information Processing Sys-

tems, Barcellona, NIPS Foundation, 2016, 1, che evidenzia come l'art. 1 del Regolamento stabilisce che la disciplina ivi contenuta « protegge le libertà e i diritti fondamentali delle persone fisiche ».

discriminatori per l'individuo che trovino la propria origine in una cieca fiducia nell'utilizzo degli algoritmi ¹⁹.

In maniera innovativa rispetto al passato, gli articoli 13 e 14 del Regolamento stabiliscono che nell'informativa rivolta all'interessato venga data notizia dell'eventuale esecuzione di un processo decisionale automatizzato, sia che la raccolta dei dati venga effettuata direttamente presso l'interessato sia che venga compiuta in via indiretta. Una garanzia di particolare rilievo viene riconosciuta allorché il processo sia interamente automatizzato essendo richiesto, almeno in simili ipotesi, che il titolare debba fornire « informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato » ²⁰. In questo senso, è utile notare come il legislatore europeo abbia inteso rafforzare il principio di trasparenza che trova centrale importanza all'interno del Regolamento. Non risulta del tutto chiaro, però, quale sia stata la ragione che ha condotto il legislatore a circoscrivere le suddette garanzie ai soli casi di processi decisionali interamente automatizzati, escludendo dalla previsione le ulteriori ipotesi in cui ci si avvale di algoritmi per giungere ad una decisione, perdendo dunque l'occasione di estendere anche a quest'ultime un più alto livello di garanzia.

L'interesse conoscitivo della persona è ulteriormente tutelato dal diritto di accesso riconosciuto dall'articolo 15 del Regolamento che contempla, a sua volta, la possibilità di ricevere informazioni relative all'esistenza di eventuali processi decisionali automatizzati ²¹. L'articolo 15, diversamente dagli articoli 13 e 14, ha il pregio di prevedere un diritto azionabile dall'interessato e non un obbligo rivolto al titolare del trattamento, e permette inoltre di superare i limiti temporali posti dagli articoli 13 e 14, consentendo al soggetto di acquisire informazioni anche qualora il trattamento abbia avuto inizio, stia trovando esecuzione o abbia addirittura già prodotto una decisione ²².

¹⁹ L'attenzione ai processi automatizzati e ai pericoli per l'individuo non era assente nella Direttiva 95/46/CE come rilevato in F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016, 92 ss.

²⁰ Cfr. artt. 13, par. 2, lett. f), e 14, par. 2, lett. g) del Regolamento (UE) 2016/679. L'indicazione all'interno dell'informativa circa lo svolgimento o meno di processi decisionali automatizzati si configura come novità rispetto alla disciplina contenuta nella Direttiva 95/46/CE.

²¹ Cfr. art. 15, par. 1, lett. h) del Regolamento (UE) 2016/679. Si rileva che

una simile previsione fosse già contenuta nell'art. 12, lett. a) della Direttiva 95/46/CE che tuttavia, nelle ipotesi di processi decisionali interamente automatizzati, assicurava solamente la conoscenza della logica applicata al trattamento, e non anche l'importanza e le conseguenze previste per l'interessato.

Si evidenzia che l'art. 15, al pari degli artt. 13 e 14, riconoscono particolari garanzie informative all'interessato unicamente quando vengono effettuati processi decisionali interamente automatizzati, e non anche nei casi in cui è contemplato un coinvolgimento umano.

²² Sulle caratteristiche che differenziano l'art. 15 dagli artt. 13 e 14 si veda S.

3.2. *Il divieto di processi decisionali automatizzati.*

Il Regolamento affianca alle garanzie conoscitive assicurate attraverso l'informativa e il diritto di accesso, un espresso limite allo svolgimento di processi decisionali interamente automatizzati. L'articolo 22, paragrafo 1, riconosce alla persona il diritto di non essere sottoposta a decisioni automatizzate prive di un coinvolgimento umano e che, allo stesso tempo, producano effetti giuridici o incidano in modo analogo sull'individuo²³. Per comprendere correttamente quanto disposto dalla disposizione è però necessario affrontare due distinte questioni interpretative che ne aiutano a chiarire l'ambito di applicazione e la portata.

La prima questione riguardante il senso da attribuire all'espressione « decisione basata unicamente sul trattamento automatizzato » è stata chiarita attraverso l'adozione di un'interpretazione di stampo sostanzialistico. Una decisione presa unicamente attraverso un processo automatizzato, infatti, dev'essere intesa come tale, non solo ove sia escluso qualsiasi contributo umano, ma anche qualora simile contributo risulti artefatto e sia irrilevante ai fini della decisione. In tal modo viene preclusa al titolare la possibilità di aggirare la previsione dell'articolo 22, paragrafo 1, attraverso l'inserimento di un coinvolgimento umano meramente formale all'interno del processo automatizzato²⁴.

Altra questione interpretativa riguarda l'espressione « diritto di non essere sottoposto » che ha determinato notevole ambiguità circa il senso da attribuire alla portata della garanzia riconosciuta dall'articolo 22. Da un lato, potrebbe essere intesa quale proibizione rivolta al titolare del trattamento, risultando automaticamente applicabile salvo il verificarsi di precise ipotesi derogatorie previste dal legislatore. Dall'altro lato, potrebbe essere interpretata quale diritto di opposizione dell'interessato, trovando applicabilità solo al di fuori delle ipotesi derogatorie previste dal legislatore e richiedendo, inoltre, un atto formale di opposizione da parte dell'individuo. Si deve notare che, mentre la prima

WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, May 2017, 7, II, 83.

²³ Sull'argomento L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016, 266 ss. Si veda inoltre A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 242 ss.

²⁴ Così l'ARTICLE 29 WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, cit., 20-21. Allo stesso modo G. MALGIERI, G. COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, cit., 251-252. Sul tema A. MANTELLERO, *I Big Data nel quadro della disciplina europea della tutela dei dati personali*, cit., 52, che pone l'accento sul problema dell'effettivo grado di libertà del decisore umano rispetto alle indicazioni fornite dall'algoritmo.

interpretazione introduce un dovere per il titolare del trattamento e una tutela *by default* per l'interessato, la seconda interpretazione finisce per ribaltare su quest'ultimo il duplice onere di essere a conoscenza dell'esecuzione di un processo decisionale automatizzato e di far valere attivamente la propria pretesa. Al fine di meglio tutelare l'individuo, pare più opportuno sciogliere il dubbio interpretativo in favore del riconoscimento di una proibizione generale diretta al titolare del trattamento, escludendo in tal modo che la garanzia prevista dall'articolo 22 possa essere compromessa dalla disinformazione o dall'inerzia dell'interessato ²⁵.

In ogni caso il Regolamento, anche con l'intento di assicurare al titolare una certa flessibilità di scelta nella gestione dei trattamenti, stabilisce tre specifiche deroghe alla proibizione generale sopra descritta. Un processo decisionale interamente automatizzato, dunque, può trovare attuazione laddove sia necessario per la conclusione o l'esecuzione di un contratto, sia autorizzato da una norma di legge oppure si fonda sul consenso esplicito del soggetto interessato ²⁶. Rispetto a quest'ultima eccezione, possono sorgere talune perplessità in merito all'effettiva tutela garantita attraverso l'istituto del consenso.

Si deve prendere coscienza, infatti, di come il consenso risulti talvolta uno strumento di per sé inidoneo a tutelare a pieno l'individuo, soprattutto ove venga utilizzato per regolare contesti complessi che prevedano l'utilizzo di algoritmi e di processi decisionali automatizzati. In più circostanze il consenso potrebbe non risultare effettivamente libero ed informato in ragione della difficoltà conoscitiva dell'individuo, il quale si interfaccia di continuo con una pluralità di trattamenti e di richieste di consenso e che, inoltre, non è sempre in grado di comprendere a pieno l'informativa che gli viene presentata ²⁷. Laddove manchi una reale consapevolezza da parte dell'interessato, rintracciare

²⁵ Si veda S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, cit., 94 ss., che indicano come una simile ambiguità interpretativa già sussisteva rispetto all'art. 15 della Direttiva 95/46/CE e che auspicano, inoltre, il superamento della suddetta ambiguità prima della diretta applicabilità del Regolamento (UE) 2016/679. Sul punto è intervenuto l'ARTICLE 29 WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, cit., 19-20, il quale ha chiarito la natura di proibizione dell'art. 22, par. 1 del Regolamento.

²⁶ Cfr. art. 22, par. 2, del Regolamento (UE) 2016/679. Si noti la natura patetica delle deroghe stabilite alle lettere a) e c).

²⁷ Si veda L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For*, in 16 *Duke Law & Technology Review* 18, 2017, 36 ss. Sull'argomento F. BRAVO, *Il consenso e le altre condizioni di liceità*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 138 ss., il quale osserva come il consenso rischi di veder erosa la propria centralità tra le condizioni di liceità del trattamento dei dati

nel semplice consenso una deroga al divieto di essere sottoposto a processi decisionali interamente automatizzati potrebbe configurare una vulnerabilità per l'individuo che finirebbe per esercitare solo un'apparente libertà di autodeterminazione informativa.

Ad ogni modo, si noti che le criticità caratterizzanti l'istituto del consenso e, più in generale, i rischi per l'individuo che emergono nelle ipotesi di deroga pattizia al divieto di processi decisionali interamente automatizzati, possono intendersi stemperate dalle garanzie inderogabili sancite all'articolo 22, paragrafo 3 del Regolamento. Infatti, nel caso di trattamenti automatizzati che risultino necessari per ragioni contrattuali o si basino sul consenso espresso, alla tutela conoscitiva prevista dagli articoli da 13 a 15 se ne affianca una ulteriore che riconosce all'interessato « il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione »²⁸.

3.3. *Right to explanation, DPIA e categorie particolari di dati.*

Le disposizioni in materia di processi decisionali automatizzati sin ora analizzate hanno concorso ad aprire una disputa dottrinale circa la possibilità di ravvisare all'interno della normativa europea il riconoscimento di un *right to explanation*. Per comprendere quale sia il contenuto di un simile diritto è utile distinguere la tipologia di spiegazione che può essere fornita all'interessato. Da un lato a seconda che la spiegazione sia data prima o dopo il raggiungimento della decisione, e dall'altro lato a seconda che abbia ad oggetto le modalità di funzionamento del processo automatizzato oppure le specifiche cause che hanno condotto alla singola decisione.

personalì. Si rileva inoltre che le criticità emergenti rispetto all'istituto del consenso trovano una possibile radice nel momento di sottoposizione dell'informativa all'interessato. Al riguardo F. H. CATE, *The Failure of Fair Information Practice Principles*, in J. K. WINN (a cura di), *Consumer protection in the age of the information economy*, Aldershot, Ashgate, 2006, 360 ss., indica alcune cause della mancata lettura dell'informativa da parte degli interessati come, a titolo esemplificativo, una generale tendenza ad ignorarle oppure il mancato raggiungimento del destinatario. Ancora, l'Autore evidenzia che problemi di comprensibilità dell'informativa possono derivare dalla complessità e dall'estremo tecnicismo con cui viene redatta. Sull'argomento L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati per-*

sonali, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017, 54 ss., che riconosce i limiti del consenso derivanti dalle innovative modalità di riutilizzo dei dati e che, parallelamente, identifica nel principio di *accountability* e negli istituti ad esso affini un consapevole tentativo di rafforzare le tutele assicurate all'individuo.

²⁸ Cfr. art. 22, par. 3, lett. a) e c) del Regolamento (UE) 2016/679. In merito alla modalità attraverso cui far valere le garanzie previste, se in maniera unitaria o meno, si veda S. WATCHER, B. MITTELSTAND, C. RUSSELL, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 6 October 2017, 35-36, reperibile in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289.

Nel sostenere l'esistenza di un *right to explanation* nel Regolamento, parte della dottrina ha affermato che la nuova normativa riconosce il diritto di ricevere una spiegazione *ex post* attraverso cui vengano illustrate le ragioni concrete che hanno determinato una specifica decisione ²⁹.

Una prima enucleazione del *right to explanation* ha trovato le basi nella previsione degli articoli 13 e 14 in materia di informativa all'interessato, ove viene richiesto al titolare di fornire informazioni significative riguardanti la logica utilizzata nel processo automatizzato e le possibili conseguenze nei confronti dell'individuo. La limitazione temporale delle disposizioni sopra richiamate, che trovano applicazione in un momento antecedente a quello in cui la decisione viene presa, unitamente all'assenza di un'espressa previsione letterale al riguardo, escludono, a parere di chi scrive, la tenuta di una simile ricostruzione.

Allo stesso modo, non pare sostenibile l'enucleazione di un *right to explanation* sulla base del diritto di accesso previsto dall'articolo 15. Nonostante quest'ultima tesi superi l'impedimento cronologico degli articoli 13 e 14, potendo il diritto di accesso essere esercitato senza limite di tempo, continua a non essere presente alcun cenno ad una spiegazione circa la decisione conseguita. Al contrario, il tenore letterale dell'articolo 15, riferendosi alla logica utilizzata e alle conseguenze previste del trattamento, concorre a circoscrivere il diritto dell'interessato ad una spiegazione *ex ante* delle modalità di funzionamento del processo automatizzato.

Una terza ricostruzione è stata sostenuta sulla base del combinato disposto tra le garanzie previste dall'articolo 22, paragrafo 3, ed il Considerando 71 del Regolamento contenente l'unica enunciazione espressa di un *right to explanation ex post* della

²⁹ Nel senso di un attuale riconoscimento del *right to explanation* si veda B. GOODMAN, S. FLAXMAN, *European Union regulations on algorithmic decision-making and a "right to explanation"*, arXiv, in <http://arxiv.org/abs/1606.08813>, 2016, 6 ss. Un'impostazione dotata di maggiore flessibilità si ha in A. D. SELBST, J. POWLES, *Meaningful information and the right to explanation*, in *International Data Privacy Law*, November 2017, 7, IV, 233 ss. In senso contrario, e come condiviso da chi scrive, S. WACHTER, B. MITTELSTADT, L. FLORID, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, cit., 76 ss., i quali sostengono che, al momento, non sia riconosciuto formalmente un *right to explanation* nel nuovo Regolamento e che piuttosto possa essere individuato un

semplice *right to be informed*. Quest'ultima tesi, più di recente, ha trovato sostegno in base a quanto è stato indicato dall'ARTICLE 29 WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, cit., 25 ss. Elemento indicativo della non sussistenza, ad oggi, di un *right to explanation ex post* sulla specifica decisione è l'assenza di un qualche riferimento al riguardo all'interno delle *good practices* fornite dalle richiamate Linee guida. La complessità interpretativa attorno alla possibile configurabilità del diritto ad una spiegazione *ex post* emerge inoltre in O. SESSO SARTI, *Profilazione e trattamento dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017, 615 ss.

decisione conseguita³⁰. Malgrado ciò, anche quest'ultima teoria non pare accettabile dal momento che trova sostegno in una previsione, quella del Considerando, a cui è attribuito un valore meramente orientativo ed in alcun modo vincolante. Una previsione che, per di più, trova i suoi contenuti interamente riprodotti negli articoli del Regolamento, eccezion fatta proprio per il diritto ad ottenere una spiegazione circa la specifica decisione conseguita.

Quanto emerso lascia ipotizzare una precisa volontà del legislatore europeo di non riconoscere, almeno in una fase iniziale, un *right to explanation ex post*, affermando la sola sussistenza del diritto a ricevere informazioni sulle logiche utilizzate nei processi automatizzati.

Il Regolamento prevede ulteriori tutele a completamento del quadro di garanzie che trovano applicazione laddove vengano utilizzati algoritmi per prendere decisioni che impattino sull'individuo. In considerazione dell'elevato pericolo per i diritti e le libertà della persona, l'esecuzione di processi decisionali automatizzati rientra in una delle ipotesi a cui la nuova disciplina lega obbligatoriamente lo svolgimento di una valutazione d'impatto preventiva (cd. *Data Protection Impact Assessment* o DPIA), finalizzata a garantire una più attenta tutela nelle ipotesi in cui il trattamento possa presentare notevoli profili di rischio per gli interessati³¹.

Anche l'elaborazione attraverso processi decisionali automatizzati delle particolari categorie di dati personali disciplinate dall'articolo 9 trova stringenti limitazioni in ragione della particolare intensità del pregiudizio che può derivare all'individuo³². Senz'altro risulta positiva l'individuazione di una tutela rafforzata laddove siano processati dati riguardanti la sfera intima della persona. Ciononostante bisogna osservare che nel contesto dell'elaborazione automatica dei dati il confine tra dato personale comune e dato particolare può risultare estremamente labile. In questo senso, è necessario che venga svolta un'attenta riflessione su cosa debba essere inteso per dato particolare, non circoscri-

³⁰ Cfr. Considerando 71 del Regolamento (UE) 2016/679: « In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione ».

³¹ Cfr. art. 35, par. 3, lett. a) del Regolamento (UE) 2016/679. Si veda ARTICLE 29 WORKING PARTY, *Guidelines on Auto-*

mated individual decision-making and Profiling for the purposes of Regulation 2016/679, cit., 29 ss., in cui si evidenzia la connessione tra esecuzione di processi decisionali automatizzati e valutazione d'impatto preventiva, sia nelle ipotesi in cui il processo sia interamente automatizzato sia in quelle in cui è contemplato un coinvolgimento umano. Così O. SASSO SARTI, *Profilazione e trattamento dei dati personali*, cit., 615 ss.

³² Cfr. Considerando 71 e art. 22, par. 4, del Regolamento (UE) 2016/679.

vendo la nozione ai soli dati direttamente rivelatori di informazioni sensibili, ma cercando di ricomprendere tutte quelle ipotesi in cui simili informazioni siano prodotte dall'elaborazione e dall'interoperabilità di dati personali comuni ³³.

4. RIFLESSIONI CONCLUSIVE.

Il Regolamento (UE) 2016/679 fornisce un importante contributo alla tutela dell'individuo all'interno del nuovo mondo digitale e, si auspica, possa concorrere alla realizzazione di soluzioni internazionalmente condivise rispetto a fenomeni che hanno assunto oggi una dimensione globale ³⁴. L'intervento normativo mostra di avere contezza dei pericoli connaturati nell'utilizzo di processi decisionali automatizzati e di essere consapevole dei potenziali trattamenti discriminatori connessi all'illusoria neutralità degli algoritmi. Nonostante ciò, non bisogna intendere il nuovo quadro normativo come un punto di arrivo che non richieda ulteriori modifiche e integrazioni. Al contrario, risulta indispensabile che taluni aspetti del Regolamento vengano sviluppati attraverso l'impegno congiunto di scienza giuridica e prassi applicativa.

In primo luogo pare opportuno che l'attività interpretativa si sforzi di enucleare quanto prima un *right to explanation* integrale, che non si limiti ad una spiegazione *ex ante* delle logiche seguite dall'algoritmo, ma che contestualmente fornisca una spiegazione *ex post* circa la specifica decisione raggiunta attraverso il processo automatizzato. A tale scopo, un'interpretazione sistematica degli articoli da 13 a 15 e dell'articolo 22 del Regolamento, unitamente ad una valorizzazione di quanto previsto dal Considerando 71, potrebbero favorire l'enucleazione di un *right to explanation* che si spinga oltre all'astratta indicazione dei criteri utilizzati ed illustri le ragioni concrete su cui si fonda la singola

³³ Così B. W. GOODMAN, *A step towards accountable algorithms?: algorithmic discrimination and the european union general data protection*, cit., 2 ss., che ad un'interpretazione restrittiva di dato particolare, secondo cui il dato contiene di per sé un'informazione sensibile dell'interessato, contrappone un'interpretazione estensiva, secondo cui il dato risulta particolare se, da solo o incrociato con altri, denota una significativa relazione statistica tra un'informazione sensibile e l'interessato. Secondo l'Autore, se la prima interpretazione è inefficace, la seconda presenta forti criticità per una completa ed effettiva attuazione. Si veda ARTICLE 29 WORKING PARTY, *Guidelines on Automated individual decision-making and*

Profiling for the purposes of Regulation 2016/679, cit., 15. Al riguardo L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For*, cit., 36 ss., che riporta il caso di un incrocio di dati personali comuni compiuto da un supermercato al fine di individuare i soggetti in uno stato di gravidanza. Simile elaborazione di dati ha portato ad identificare la gravidanza di una ragazza ancor prima che ne avessero consapevolezza i familiari.

³⁴ In tal senso C. KUNER, D. JERKER, B. SVANTESSON, F. H. CATE, O. LYNKEY, C. MILLARD, N. N. LOIDEIAN, *The GDPR as a chance to break down borders*, in *International Data Privacy Law*, November 2017, 7, IV, 231 ss.

decisione³⁵. Simile impostazione, per altro, risulterebbe coerente con i principi di trasparenza e di *accountability* che permeano l'intero Regolamento, assicurando una maggiore visibilità dell'algoritmo e favorendo l'effettiva appellabilità delle decisioni da parte dei soggetti direttamente interessati dal processo automatizzato.

Fintantoché l'evoluzione della disciplina non approdi al riconoscimento di un *right to explanation* integrale, può risultare utile adottare modalità semplificate attraverso cui spiegare la logica seguita dal processo decisionale. In particolare, si potrebbe fornire una spiegazione controfattuale che descriva quale sia la dipendenza da fattori esterni idonea ad assumere un ruolo determinante all'interno della decisione. Con grande efficacia esemplificativa, questo modello di spiegazione presenterebbe il vantaggio di acquisire concretezza, di garantire maggiore prossimità rispetto alla decisione del caso di specie e di indicare all'interessato l'aspetto concreto su cui intervenire affinché in futuro la decisione possa essergli favorevole.

La linearità e l'immediatezza della spiegazione consentirebbe di superare le obiezioni sollevate in nome del diritto di proprietà intellettuale invocato a tutela della segretezza del modello matematico, poiché non sarebbe necessario illustrare in modo puntuale il funzionamento dell'algoritmo né tantomeno risulterebbe necessario svelarne il codice. Verrebbe assicurata una maggiore semplicità del processo decisionale a vantaggio degli interessati attraverso una spiegazione che, pur rivolgendosi ad una platea vasta ed eterogenea, risulti chiara e da tutti facilmente comprensibile³⁶.

Gli interventi volti a garantire un adeguato livello di tutela dell'individuo non si devono esaurire nella sola regolamentazione delle modalità con cui eseguire processi automatizzati. Bisogna prevedere un intervento che disciplini e vigili sull'attività dei soggetti coinvolti in prima persona nello sviluppo degli algoritmi,

³⁵ L'impulso per una riflessione finalizzata alla valorizzazione del *right to explanation ex post* enunciato dal Considerando 71 può essere ravvisata in ARTICLE 29 WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, cit., 27. La centralità del valore interpretativo da riconoscere ai Considerando è evidenziata in C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale

Scientifica, 2017, 90-91, cosicché l'interpretazione del testo del Regolamento tenga conto delle ragioni e delle esigenze alla base dell'intervento normativo.

³⁶ Sul tema delle *counterfactual explanations* si veda S. WATCHER, B. MITTELSTAND, C. RUSSELL, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, cit., 5 ss. e 22 ss. A titolo esemplificativo gli Autori indicano che una spiegazione controfattuale possa essere espressa come segue: « *You were denied a loan because your annual income was £30,000. If your income had been £45,000, you would have been offered a loan* ».

i *Data Scientists*, poiché sono quest'ultimi che, nel definire gli obiettivi e le logiche dei processi matematici, dettano in concreto le regole attraverso cui gli algoritmi plasmano il mondo ed incidono sulle nostre vite. Da un lato, dunque, si potrebbe ipotizzare l'adozione di codici di condotta che fissino regole condivise ed omogenee per i *Data Scientists*. Dall'altro lato, si potrebbe valutare la formazione di apposite figure di controllo e monitoraggio che abbiano il compito di svolgere attività di *audit* sull'utilizzo di algoritmi all'interno di processi decisionali.

Risulta opportuno, inoltre, avviare una valutazione critica che abbia ad oggetto i principi cardine della disciplina a protezione dei dati personali e che approfondisca, in modo particolare, la loro capacità di governare efficacemente le dinamiche che caratterizzano il mondo digitale.

I rischi connessi all'impiego di processi automatizzati, i quali possono avere un impatto non circoscritto alla sola sfera della protezione dei dati personali, suggeriscono che prima dell'esecuzione di un'attività di trattamento ne venga accertata la conformità ai valori etici e sociali generalmente condivisi. Una valutazione da svolgere nella fase preliminare rispetto all'avvio del trattamento e che può integrare in modo innovativo la DPIA introdotta dall'articolo 35 del Regolamento³⁷. In tal modo la responsabilizzazione dei titolari e dei responsabili non si limiterebbe a considerazioni riguardanti i soli profili tecnici e giuridici del trattamento ma, attraverso la realizzazione di un *Privacy, Ethical and Social Impact Assessment* (cd. PESIA)³⁸, si arricchirebbe di una più ampia riflessione circa le potenziali conseguenze etiche e sociali derivanti dall'utilizzo dei dati. In ragione della relatività connaturata alla dimensione etica e sociale, tipicamente dipendente dal contesto spaziotemporale di riferimento, il modello PESIA intende valutare ciascun singolo caso attraverso un'architettura di valori operante su tre livelli³⁹.

In primo luogo la congruità del trattamento viene misurata

³⁷ In merito alla DPIA *supra* nota 29.

³⁸ Una riflessione *de iure condendo* sull'implementazione del modello PESIA si trova in A. MANTELERO, *Il nuovo approccio alla valutazione del rischio nella sicurezza dei dati*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 326 ss. L'Autore, pur riconoscendo i maggiori oneri di costi e risorse connessi all'adozione del modello PESIA, segnala l'opportunità di una sua implementazione attraverso una valutazione complessa e articolata che venga svolta da esperti di più aree scientifiche, non circoscritte all'ambito giuridico ed informatico.

Così A. MANTELERO, *I Big Data nel quadro della disciplina europea della tutela dei dati personali*, cit., 56 ss.

³⁹ Cfr. CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, Strasburgo, 23 Gennaio 2017, 3-4. Le Linee guida, pur facendo parte dell'attività normativa del Consiglio d'Europa non direttamente connessa all'adozione del Regolamento (UE) 2016/679, possono diventare un utile punto di riferimento ai fini di una futura implementazione del modello PESIA.

rispetto ai valori etici e sociali comuni, identificabili in modo pacifico nei valori affermati all'interno delle Carte internazionali a tutela dei diritti e delle libertà fondamentali della persona. Inoltre, per calibrare la valutazione al contesto specifico, il modello PESIA tiene in particolare considerazione i valori condivisi dalla comunità a cui appartiene l'individuo e, da ultimo, esamina gli specifici valori coinvolti nel caso di specie al fine di definire un inquadramento di dettaglio. L'adozione di un approccio etico-sociale potrebbe assicurare maggiore completezza alla tutela garantita all'individuo e fornirebbe l'opportunità di considerare gli effetti connessi all'elaborazione dei dati in una prospettiva collettiva, non limitata al singolo soggetto sottoposto al trattamento.

Proprio la valorizzazione della prospettiva collettiva potrebbe dare impulso ad una riflessione che si interroghi sulla dimensione riconosciuta al diritto alla protezione dei dati personali. L'impostazione atomistica adottata sin ora e ribadita all'interno del Regolamento può risultare talvolta riduttiva in considerazione delle innovative modalità di elaborazione dei dati⁴⁰. Ciò ha condotto parte della dottrina a sviluppare il concetto di *group privacy*⁴¹ che, parallelamente al riconoscimento di un diritto soggettivo individuale, valorizzi la dimensione collettiva della privacy. Si deve osservare, infatti, che l'utilizzo di algoritmi e di processi automatizzati ha modificato radicalmente le metodologie attraverso cui i dati vengono elaborati e vengono prese decisioni. Ci si focalizza non sul singolo individuo ma sull'identificazione di gruppi che presentano caratteristiche comuni e nei quali il singolo viene di volta in volta inserito (cd. gruppi *ad hoc*)⁴².

L'elemento essenziale non è tanto l'identificabilità della speci-

⁴⁰ Nonostante la nuova disciplina mantenga un'impostazione atomistica, si deve osservare che il Regolamento riconosce il diritto alla protezione dei dati personali non solo quale diritto dell'individuo ma anche come interesse pubblico europeo, tutelabile autonomamente rispetto alle esigenze di protezione del singolo. Simile impostazione si evince dalla previsione del Considerando 4, secondo cui « Il diritto alla protezione dei dati di carattere personale (...) va considerato alla luce della sua funzione sociale », e dagli articoli 24, 33, 34, 80, 83 e 84 del Regolamento. Al riguardo si veda F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, Giappichelli, 2016, 4-5.

⁴¹ Il concetto di *group privacy*, che ancora non trova una definizione univoca e pacifica, si propone di estendere ad un determinato gruppo, da intendersi non quale somma dei singoli membri ma come gruppo

in sé, il diritto ad un'identità informazionale inviolata. Sull'argomento B. MITTELSTADT, *From Individual to Group Privacy in Big Data Analytics*, in *Philosophy & Technology*, December 2017, 30, IV, 477 ss. Il tema è affrontato sotto molteplici profili in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Springer, 2017.

⁴² I gruppi *ad hoc* si differenziano sia dai gruppi che si formano intenzionalmente per unione comune, come ad esempio i sindacati, sia dai gruppi la cui unione non è intenzionale ma è frutto di un legame ereditato, come ad esempio i gruppi etnici. I gruppi *ad hoc* sono creati e modificati di continuo attraverso una classificazione algoritmica ed in base agli obiettivi di terze parti. In tali gruppi non è riscontrabile alcuna volontà o sentimento di aggregazione tra i membri i quali, il più delle volte, sono del tutto inconsapevoli di essere ricompresi in uno o più gruppi. Così B. MITTELSTADT,

fica persona, quanto piuttosto l'individuazione degli aspetti (comportamenti, preferenze, ecc.) che accomunano i vari individui e sulla base dei quali è possibile raggrupparli⁴³. Dalla formulazione dei gruppi *ad hoc* e dal loro utilizzo attraverso processi decisionali automatizzati si possono dunque determinare trattamenti discriminatori di ampia portata che vadano ad incidere sul gruppo individuato e, in via indiretta, su quei soggetti che, anche se non identificati, vi sono ricompresi. Per tale ragione risulta opportuno elaborare nuovi modelli a tutela della privacy che non siano unicamente incardinati sulla protezione del singolo individuo e che tengano conto della classificazione in gruppi sempre più utilizzata all'interno dei processi automatizzati.

Si coglie nella disciplina del Regolamento (UE) 2016/679 la consapevolezza del delicato momento storico in cui si trova l'essere umano. L'intervento normativo ha il merito di offrire utili indicazioni sulle modalità attraverso cui regolare il nuovo mondo digitale, fornendo un contributo importante ma non esaustivo per rispondere alle criticità connesse all'innovazione tecnologica. Quella del Regolamento, dunque, deve essere intesa quale disciplina minima da integrare e sviluppare nel tempo da parte del legislatore e, ancor prima, dalla prassi applicativa che dovrà mostrarsi capace d'interpretare in modo quanto più garantistico il quadro normativo appena delineato.

Le rivoluzioni necessitano di tempo per essere pienamente assimilate. Come è successo per la rivoluzione industriale, l'obiettivo a cui bisogna tendere non è quello di rinunciare all'innovazione tecnologica, ma è quello di ricalibrare i diritti e le libertà della persona in base al mutato contesto e alle criticità emergenti. Tuttavia, se per l'adeguamento alla rivoluzione industriale si sono avuti a disposizione secoli, la sfida con cui bisogna confrontarsi oggi è quella di raggiungere nell'arco di pochi anni un contemperamento tra l'efficienza tecnologica e la tutela dell'individuo. Un bilanciamento che accolga i vantaggi connessi all'utilizzo degli algoritmi e che, allo stesso tempo, valorizzi il coinvolgimento umano e preservi i diritti fondamentali della persona, sia come singolo sia nella sua dimensione di gruppo.

From Individual to Group Privacy in Big Data Analytics, cit., 484 ss.

⁴³ A titolo esemplificativo: non è essenziale sapere che il soggetto X corrisponde a Tizio ma è di centrale importanza sapere che il soggetto X rientra nel gruppo *ad hoc* che ha come elementi caratterizzanti la passione per il teatro, il consumo di bevande alcoliche e l'abitudine di trascorrere i mesi estivi in montagna. In questo senso L. FLORIDI, *Group Privacy: A Defence and an Interpretation*, in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura

di), *Group Privacy. New Challenges of Data Technologies*, Springer, 2017, 98, rileva che « *users of big data may not care about Alice at all, but only about the fact whether Alice, whoever she is, belongs to the group that regularly goes to the local church, or mosque, or synagogue, uses Grindr, or has gone to a hospital licensed to carry out abortions, or indeed shares a feature of your choice. In military terminology, Alice is hardly ever a High Pay-off Target, like a tank in a column of tanks. It is the column that matters* ».