ISSN 2281-5147

Opinio Juris in Comparatione

Studies in Comparative and National Law

Vol. 1, n. 1/2018

La profilazione di gruppo: ombre della nozione di "personalità del dato"

Giorgia Bucaria

Pacini Giuridica

La profilazione di gruppo: ombre della nozione di "personalità del dato"

Giorgia Bucaria*

Abstract

Questo contributo si apre con una nota metodologica: la valutazione del grado di efficacia di uno strumento normativo non può prescindere da una indagine preliminare sull'adeguatezza del suo campo di applicazione. Di conseguenza, al fine di poter giudicare dell'efficacia del GDPR, si analizzerà l'adeguatezza della nozione di "personalità del dato", in quanto criterio di attivazione dell'applicazione del Regolamento. Dopo aver evidenziato le contraddizioni interne a questo concetto, ci concentreremo sul caso della profilazione di gruppo, ambito in cui le conseguenze delle problematicità esposte nei paragrafi precedenti emergono con maggior forza. A tal proposito, si tenterà di aprire una nuova via che possa stemperare alcune delle problematicità esposte. La non-personalità dei dati utilizzati in quest'ambito, infatti, impedisce l'applicazione del GDPR dopo la generazione dei profili di gruppo. Tuttavia, le precedenti fasi del trattamento sono soggette alle regole e alle tutele del GDPR e, in particolare, all'art. 35, che potrebbe essere utilizzato per impedire, o quantomeno mitigare a priori, le conseguenze più dannose di tale pratica. Infine, tornando alla domanda di partenza sull'efficacia del Regolamento, concluderemo con una riflessione generale sulla coerenza tra la portata applicativa del GDPR e i gli obiettivi di policy da questo dichiarati.

Parole Chiave

Personalità del Dato – Profilazione di Gruppo – Algoritmi – Discriminazione – DPIA

* Honor Student, Sant'Anna School of Advanced Studies.

Table of contents:

Introduzione: il GDPR e la sua applicabilità

Il Regolamento Europeo in materia di protezione dei dati personali (GDPR, secondo il suo acronimo in inglese)[1] ha l'onore e il merito di avere colorato di efficacia normativa il più avanzato e moderno sistema di tutela dei dati personali ad oggi esistente. Il nuovo regolamento, senza dubbio, offre ai soggetti sottoposti al trattamento dei dati personali un inedito intreccio di regole puntuali e clausole generali in grado di ricomporre, nelle pieghe dei principi elencati dall'art. 5[2], le irrinunciabili istanze di tutela personalistica dell'interessato[3] e le innegabili esigenze di efficienza del titolare del trattamento, in particolare, e del mercato, in generale[4]. Si considera, però, opportuno preoccuparsi, prima che della validità delle *modalità applicative* degli strumenti giuridici che il Regolamento propone, dell'adeguatezza del loro *campo di applicazione*. Un tale ragionare, del resto, è del tutto conforme al normale svolgersi dell'attività giuridica: in prima istanza si procede alla sussunzione del fatto nella fattispecie – operazione che mai potrebbe svolgersi senza una preliminare indagine sulle condizioni di applicabilità della regola – e, solo dopo, il

[1] Reg. EU 2016/679, 27 aprile 2016, GU L 119.

[2] Art. 5, Reg. EU 2016/679, cit.

[3] Senza dubbio, l'istanza di tutela personalistica è prevalente. Basti guardare alla nomenclatura sotto cui cade il regolamento: «[…]relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali […]».

[4] A tal proposito, i conss. 2 e 4 del GDPR (Reg. EU 2016/679, cit.) annoverano, tra le finalità del GDPR, la «realizzazione di uno spazio di libertà, sicurezza e giustizia», il «benessere delle persone fisiche», ma anche il «progresso economico» e il «rafforzamento e [...] la convergenza delle economie nel mercato interno» (cons. 2, *ivi*). Il diritto alla protezione dei dati, infatti, non è una «prerogativa assoluta», ma va realizzato «alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali» (cons. 4, *ivi*). Sui benefici economici che derivano dal trattamento dei dati personali, si veda: EU Commission, Factsheet: "The EU Data Protection Reform and Big Data", aprile 2015; EU Commission, Communication: "Building a European data economy", 10 gennaio 2017.

giurista potrà affrontare il problema successivo, ossia le modalità, i meccanismi, le problematicità tecniche poste dalla concreta applicazione. Lo scopo di questo contributo, dunque, muove dalla consapevolezza che un'indagine preliminare sull'applicabilità della norma – *quali* fatti essa regoli piuttosto che *come* essi siano regolati – sia assolutamente dirimente nella definizione del grado di efficacia di un *corpus normativo* e che una tale valutazione sia da farsi anzitutto sulla congruenza dell'ampiezza della sua portata rispetto alla *ratio* dello stesso. Dunque, prima di richiamare l'attenzione sugli strumenti di tutela offerti dal Regolamento e di proporre interpretazioni e soluzioni circa le difficoltà pratiche della loro applicazione, bisognerà riflettere sull'ampiezza del loro "*an*" e sulla adeguatezza della loro applicabilità. In questa sede, dunque, ci si concentrerà sull'ambito applicativo del GDPR per verificare se i criteri della sua applicabilità siano effettivamente idonei ad implementare la *ratio* che lo ispira. Tale domanda è, ad un sol tempo, *collaterale*, nel senso che è ben possibile parlare del GDPR e degli strumenti di tutela che questo offre senza affrontarla, e *propedeutica* o *preliminare*, nel senso che precede – da un punto di vista logico e cronologico – ogni ulteriore questione che attiene al Regolamento. Conseguentemente, avendo detto che la valutazione dei criteri di applicabilità della norma fa perno sulla congruenza degli stessi rispetto all'obiettivo di *policy* di cui essa si incarica, la nostra analisi si snoderà in due passaggi argomentativi. Anzitutto, rifacendoci al dato normativo, dovremo definire la natura dei criteri di applicabilità, nonché la *ratio* e gli obiettivi propri del regolamento. In seguito, esamineremo le contraddizioni che emergono con maggiore forza e problematicità, notando come uno dei principali obiettivi che il Regolamento, tra gli altri, si pone – la tutela dell'identità personale – venga tradito, alla prova dei fatti, dalla definizione dei suoi confini di applicabilità.

1. Natura e *ratio* del criterio della personalità del dato: una contraddizione?

Il quesito su quali fatti attivino l'applicazione del regolamento sembrerebbe già risolto dall'art. 2, par. 1[5], che elegge il concetto di "*personalità* del dato" a criterio di discernimento tra fatti che esigono l'applicazione del GDPR e fatti che, invece, la escludono. A questo punto, è naturale interrogarsi sulla natura degli elementi costitutivi della fattispecie di "personalità del dato" o, in altre parole, sulle caratteristiche che trasformano una informazione qualunque in un *dato personale*, così permettendo l'applicazione del Regolamento. Sul punto interviene la definizione di "dato *personale*" di cui all'art. 4(1), per cui un dato si considera "personale" ogni qual volta esso si presenti come una «qualsiasi informazio-

[5] Art. 2, par. 1, Reg. EU 2016/679, cit.: «il presente regolamento si applica al trattamento […] di dati personali […]».

ne riguardante una persona fisica identificata o identificabile[6]». Nel documento emanato in proposito, l'*Article 29 Working Party* (WP29) scompone la nozione di *personalità* in quattro distinti elementi[7], la cui presenza cumulativa consente di qualificare un dato come personale e, dunque, di applicare le tutele offerte dal GDPR. Dunque, la "personalità del dato" sussiste a queste quattro condizioni: quando si è in presenza di una *qualsiasi informazione*, quando tra detta informazione e il soggetto interessato è possibile riscontrare un legame (di «contenuto, […] scopo […] o risultato[8]») tale da consentirci di affermare che l'informazione *riguardi* detto soggetto, quando quest'ultimo sia *una persona fisica* e, infine, quando questa risulti *identificata o identificabile*. In aggiunta, dall'esame del documento[9], emergono due ulteriori requisiti, impliciti nel concetto di "identificabilità": la "distinguibilità" e la "singolarità" della persona soggetta alla relazione di *contenuto*, *scopo* o *risultato*. La necessità della "distinguibilità" del soggetto emerge dall'equazione che il WP29 pone tra "identificazione" del soggetto e "distinzione" dello stesso, nel senso che «si può considerare 'identificata' la persona fisica che, all'interno di un gruppo, è "distinta" da tutti gli altri membri[10]». Il requisito della "singolarità", invece, si ricava dalla nozione stessa di *persona fisica,* in cui, chiaramente, un gruppo non è ricompreso. A partire da questi dati – e procedendo *a contrario* – si giunge alla conclusione che, in mancanza di uno solo di questi elementi costitutivi, il GDPR non trovi margini di applicazione. Va, dunque, ammesso che esiste un'area residuale di informazioni (dati *non* personali) che, non *riguardando* alcuna persona fisica identificata o identificabile, sono irrimediabilmente al di fuori dell'ambito di applicazione materiale del GDPR. Si è parlato, a tal proposito, di dati non riguardanti alcun "*data-subject*", ma inerenti a "*data-points*", ovverosia sorgenti di dati che non si presentano come "una persona fisica identificata o identificabile" [11].

A voler indagare le ragioni di politica legislativa[12] che sottendono alla scelta di siffatto criterio, queste appaiono come l'ovvia conseguenza della volontà del legislatore di imple-

[6] Art. 4(1), Reg. EU 2016/679, cit.

[7] Art. 29 Working Party, WP 136, *Parere 4/2007 sul concetto di dati personali*, 20 giugno 2007, pp. 6 e ss.

[8] *Ibid*.

[9] *Ibid*.

[10] WP 136, *cit*., 13. Ma anche, *ivi*: «identificare una persona – cioè distinguerla – […]. Attraverso gli identificatori l'informazione originale viene associata a una persona fisica che può essere distinta da altri individui. […] Si può […] considerare […] la persona "identificabile" perché […] le informazioni […] consentiranno di distinguerla dalle altre».

[11] Si veda la distinzione [J. van den Hoven, *Information Technology, Privacy and the Protection of Personal Data*, in J. van den Hoven – J. Weckert, et al. (a cura di), *Information Technology and Moral Philosophy*, Cambridge, 2008, 301-332] tra «*referential data*» e «*attributive data*» (*Ivi*, p. 309), con ciò ad intendere che la *personalità* dell'informazione è apprezzabile solo se è riferita ad un "individuo specifico" e non ad una "persona qualunque".

[12] Sulla *politicità* della scelta del criterio che traccia i confini di applicabilità del Regolamento si veda P. Schwartz – D.J. Solove, *The PII problem: privacy and a new concept of personally identifiable information*, in *New York University Law Rev.*, 2011, 1814-1894. Gli AA. individuano tre differenti approcci alla nozione di dato personale: un «tautological approach», un «non-public approach» e uno «specific-types approach» (p. 1829). A sentire le parole della Commissione Europea, COM (90) 314 final, 13.9.1990, p. 19 (commentary on Article 2): «a broad definition is adopted in order to cover all information which may be linked to an individual» e del WP29 (WP 136, *cit*., pp. 5 e 6: «[la] definizione [è] sufficientemente

mentare un sistema di gestione graduata del rischio[13], in grado di bilanciare le contrastanti esigenze di libertà nella circolazione dei dati e di protezione per i diritti e libertà fondamentali dei soggetti coinvolti, assecondando la duplice tensione – l'*efficienza* del mercato e la *giustizia* per il singolo[14] – che anima il Regolamento. Tutto ciò, alla luce della constatazione, tanto nitida quanto formalistica e semplificatoria, che soggetti da tutelare, in caso di mancata identificazione, non ve ne sono. Il GDPR, dunque, ha proprio qui la sua chiave di volta interpretativa e applicativa: si assume che solo *l'identificazione* sia astrattamente in grado di minacciare diritti e libertà e, conseguentemente, in tanto si giustifica la perdita di efficienza e valore aggiunto che consegue alla limitazione della libera circolazione dei dati, in quanto sussista il concreto rischio di identificare il soggetto. Eppure, la variabilità dei fenomeni che dovrebbero essere regolati da una siffatta nozione di *personalità* (e, *a contrario,* di non-personalità) si è occupata di smentire la sua adeguatezza in punto di fatto. Esiste, infatti, una *zona grigia* all'interno della quale l'equazione tra *identificazione* e *rischio* sembra perdere di aderenza alla realtà e risolversi in una contraddizione di non semplice soluzione: il GDPR, nato dall'esigenza di tutelare i diritti e le libertà degli individui in relazione ai rischi che derivano dal trattamento dei dati, aprioristicamente esclude, dal novero delle situazioni che beneficiano di una tutela giuridica, una serie di fatti che, per coerenza con la *ratio* di tutela delle persone fisiche, dovrebbero invece collocarsi all'interno delle *frontiere* della *personalità del dato*. L'assunta coincidenza tra personalità del dato e identificazione del soggetto (nel senso di ritenere che solo se il dato è *personale* sussistano rischi per i soggetti a vario titolo coinvolti) non consente di apprezzare – e conseguenzialmente proteggere – tutta quella gamma di situazioni *sfumate* che, pur in mancanza di identificazione, *de facto* creano rischi – attuali, concreti e significativi – per le personale coinvolte, non meno che nel caso in cui sussista un'effettiva identificazione di tali soggetti. Il caso in cui tale dinamica emerge in tutta la sua forza (e a cui, in questa sede, faremo specifico riferimento) è la profilazione di gruppo: pur presentando rischi del tutto assimilabili a quelli riscontrabili nel caso di profilazione individuale, la mancanza di soggetti *identificati o identificabili* – nel senso di *singolarmente distinguibili* – impedisce ogni forma di tutela per le persone coinvolte. Se efficace è lo strumento che risponde all'obiettivo per cui è stato concepito, non è un'iperbole definire questa discrasia un *gra-*

ampia da anticipare le evoluzioni e cogliere tutte le "zone d'ombra" nel suo campo di applicazione, facendo un uso legittimo della flessibilità offerta») non v'è dubbio che il Legislatore Europeo abbia optato per la prima tipologia. Eppure, un'altra *scelta politica* si impone: la povertà di contenuto delle tautologie, rende la definizione dei criteri di *personalità* del dato una questione non meno *politica* della preliminare opzione per l'approccio di tutela da seguire.

[13] Come dimostrato, in particolare, dal cons. 26, Reg. EU 2016/679, cit., che definisce la nozione di "identificazione" – e, dunque, personalità – in base ad un "criterio di ragionevolezza": non sarebbe conforme alla *duplice ratio* (*supra,* nota 4) del GDPR riferirsi all'identificabilità e all'anonimità come concetti *ab-soluti* e assolti dal raffronto con le circostanze di fatto. A tal proposito si veda anche P. Ohm, *Broken promises of privacy: responding to the surprising failure of anonymisation,* in *UCLA Law Rev.*, 2010 e M. Hintze, *Viewing the GDPR Through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency*, in *International Data Protection Law,* 2018, 86-101.

[14] Cfr. *supra,* nota 4.

vissimum vulnus alla tenuta Regolamento. Ecco, dunque, la *radicale aporia* del GDPR: esistono pratiche che sono astrattamente in grado di minacciare i diritti e le libertà delle persone fisiche e che, nonostante ciò, non svolgendosi a mezzo di dati definibili come "personali" (in mancanza del requisito dell'*identificazione*), non cadono nel suo ambito di applicazione materiale[15] *ex* art. 2[16].

2. Il caso della profilazione di gruppo: quali rischi per i soggetti coinvolti?

L'osservatorio privilegiato dei problemi fino ad ora enucleati è quella particolare tecnica di trattamento dei dati che va sotto il nome di "*profilazione di gruppo*". Questo caso è particolarmente utile per evidenziare i tratti del problema che fino ad ora ha fatto da *fil rouge* del nostro discorrere: a fronte di serissimi rischi per i soggetti coinvolti da tale trattamento, la loro non identificabilità preclude loro ogni forma protezione. Per attenerci al testo del GDPR, la profilazione è, in generale, definita come una «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica[17]». Questa si svolge tramite la generazione e successiva applicazione di un profilo, che, invece, viene definito come un'*informazione*[18] (dunque, un dato) caratterizzata da particolari procedure[19], da specifiche fi-

[15] Non soltanto la preoccupazione per i rischi enunciati ma anche la più classica logica giuridica (sintetizzabile nel brocardo "*ubi eadem ratio, ibi eadem dispositio*") spinge verso una siffatta conclusione: altrimenti, si tradirebbe il tipico ragionamento dell'*argumentum a simili*, il quale pretende, in virtù di una somiglianza rinvenuta a seguito del confronto tra due fattispecie differenti (il cd. *quid comune*, che si impernia sulla *ratio* ispiratrice della norma), di estendere ad una il regime previsto per l'altra. Tale estensione si giustifica sulla base del rinvenimento della ragione di politica legislativa sottesa alla prima fattispecie anche nella situazione che pure non è espressamente soggetta alla portata della norma. Diversamente, si sfocerebbe nell'irragionevole conclusione di rispondere in modo diverso ad esigenze similari.

[16] Art. 4(4), Reg. EU 2016/679, cit.

[17] *Ivi,* Art. 2. Tuttavia, prescindendo dalla definizione prettamente normativa, giova una ricognizione più "tecnica" dell'attività di profilazione. Sappiamo che questa si suddivide in successivi passaggi, efficacemente riassunti nella nozione di *KDD-process* (*Knowledge discovery in databases*): si assiste *in primis* alla registrazione dei dati in un formato che sia "*machine-readable*", poi alla sistemazione (*storing*) e all'aggregazione di questi dati a formare un *database*, al cui interno si scopre un *pattern* a seguito di una attività di *data-mining,* il quale, formalizzato e verbalizzato in un profilo, assume la forma di "*new applicable knowledge*", utilizzabile sulla base di *proxy* attivatrici (*activators*). Per ulteriori informazioni sul punto, si veda: U. Fayyad – G. Pia Tetsky-Shapiro – P. Smyth, *From Data Mining to Knowledge Discovery in Databases*, in *AI Magazine*, 17, 3, 1996; V. Mayer-Schönberger, K. Cukier, *Big data: a revolution that will transform how we live, work, and think*, Boston, 2013; Backhouse J, M. Hildebrandt, *D7.2: Descriptive analysis and inventory of profiling practices*, in *FIDIS Consortium*, p. 29. Disponibile su: <http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7- del7.2.profiling_practices.pdf>; M. Hildebrandt – S. Gutwirth (a cura di), *Profiling the European citizen: Cross-disciplinary perspectives*, Springer, 2008.

[18] Più precisamente, nelle parole di A. Romei, S. Ruggeri, *Discrimination Data Analysis: A Multi-disciplinary bibliography*, in B. Custers – T. Calders *et al.* (a cura di), *op. cit.:* «Profiles consists of patterns, rules, or any other form of knowledge that can be used to screen people», intendendo che i profili sono una verbalizzazione di tali *pattern*.

[19] Il WP29 (Art. 29 Working Party, WP 251, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 3 ottobre 2017, p. 7) ha riunito questi passaggi in una serie tripartita composta da una

nalità, da un inedito statuto epistemologico[20] e da innovative tecniche statistiche[21]. È facile, dunque, capire perché proprio alla profilazione[22] si imputa di aver offuscato la chiarezza della definizione di "dato personale": a fronte di una relazione "di finalità" e "di risultato" sempre presente, l'applicabilità del GDPR è, nel caso della profilazione di gruppo, esclusa dalla non-identificabilità (*non-singolarità* e *non-distinguibilità*) dei dati utilizzati.
Andando più nello specifico del caso che in questa sede di vuole analizzare, converrà cercare di discernere tra i dati che a vario titolo intervengono in tale attività, sì da poter

prima fase di raccolta dei dati (*data-collection*), un successivo momento di analisi automatizzata dei dati finalizzato alla scoperta delle correlazioni (*profile-generation*) e, in ultimo, una fase di applicazione di questa "nuova conoscenza" per determinare caratteristiche, attitudini, comportamenti di alcuni soggetti e/o selezionarli (*profile-application*).

[20] L'attività di profilazione elegge a terreno di svolgimento privilegiato il contesto dei Big Data (M. Hildebrandt (2013), *Slaves to Big Data. Or Are We?*, oi *Selected Works*, 2013, Disponibile su: <https://works.bepress.com/mireille_hildebrandt/52/>. Se, come è vero (cfr. *supra* nota 18) i profili sono verbalizzazioni di risultati di analisi statistiche, allora questi non assurgono a certezza quando viene svelata la relazione causa-effetto che vi è sottesa, come invece è nell'epistemologia classica (*rectius,* post-galileiana), ma, *sic et simpliciter*, quando il collegamento tra due eventi – a prescindere da ogni sequenzialità logica – si manifesta con una frequenza statistica sufficientemente elevata (M. Hildebrandt, *Profiling. From Data to Knowledge: The challenges of a crucial technology*, in *Datenschutz und Datensicherheit*, 2006). Nel dominio della profilazione e del *Big-Data-Mining*, il principio di causalità smette il suo ruolo di elemento "fondativo" della conoscenza per trasformarsi in un elemento di corroborazione ex-post della stessa e una conferma della sua percettibilità all'occhio umano. La "*new applicable knowledge*" formalizzata nel profilo, dunque, è da ritenersi robustamente fondata e accertata – dunque, applicabile – unicamente in virtù del principio di correlazione. Il principio di causalità, invece, da *princeps assoluto* e elemento costitutivo della conoscenza stessa, si è tramutato in un concetto eccessivamente «old-fashoned» per un'epoca che più efficacemente funziona basandosi sull' «how, when, where, depending on what, with no time to sort out the causes 'behind' the correlations» (M. Hildebrandt, *op. cit.*, 2013), tanto da portare esponenti della dottrina a proclamare «the end of theory» (C. Anderson, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete* in *Wired Magazine*. Disponibile su: <https://www.wire.com/2008/06/.pb-theory/amp>. Sul punto si veda, per tutti, G. Comandé, *The Rotting Meat Error: From Galileo to Aristotle in Data Mining*, in *EDPL*, 3, 2018.

[21] I metodi statistici di produzione di queste nuove informazioni divergono dalle procedure – per così dire – convenzionali. Nella parole del Consiglio d'Europea (Council of Europe*, Of data and men: Fundamental rights and freedoms in a world of big data,* 11 gennaio 2016, T-PD- BUR(2015)09REV), i profili si caratterizzano come «dynamic pattern» (*Ivi,* p. 10), formalizzati sulla base di correlazioni rinvenute non dall'occhio umano tra oggetti dello spazio fisico ma piuttosto tra dati esistenti solo nel mondo digitale, indipendentemente da ogni spiegazione causale. Diversamente da quanto accade nelle metodologie di analisi statistiche convenzionali, che di prassi vedono la presenza di alcune ipotesi preliminari con la funzione di indirizzare la raccolta dei dati, il contesto dei Big Data, al contrario, modula la produzione di nuova conoscenza in modo opposto: la raccolta dei dati è il primo passo su cui si fonda la generazione stessa dell'ipotesi (*Ivi*, 11. Da qui la formula «N=ALL» (M. Hildebrandt, *Slaves to Big Data. Or Are We?*, cit.): la quantità *N* di dati ottimale – ma non sarebbe nemmeno un azzardo dire la quantità minima – per portare avanti una attività di profilazione che sia precisa ed efficace al massimo grado sia "N=All data", dal duplice punto di vista quantitativo (tutti i dati possibili) e qualitativo (tutti i tipi di dati possibili, a prescindere dalla loro "personalità", come anche ha chiarito il Consiglio d'Europa, nell'annoverare la «variety» tra le principali caratteristiche dei Big Data (Council of Europe, cit., 6). Nelle parole di B. Custers, *Data Dilemmas in the Information Society: Introduction and Overview*, in B. Custers – T. Calders *et al.* (a cura di), *op. cit.*: «the sample size is a[n] […] important factor influencing certainty. […] The larger the sample size, the more certain the results». Dello stesso autore si veda anche B. Custers, *The Power of Knowledge: Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Wolf Legal Publishers, 2004, 56-58 sulla differenza tra *giustificazione* e *validazione* della conoscenza.

[22] Nelle parole del Comitato dei Ministri del Consiglio d'Europa, *Recommendation to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, 23 novembre 2010, p. 1: «profiling may thus provide benefits for users, the economy and society at large» e, dunque essere nell'interesse legittimo «of both the person who uses it and the person to whom it is applied, […] by leading to better market segmentation [...] and adapting offers to meet demand by the provision of better services» o, più in generale, permettendo di migliorare la «consumers' and users' experience» (Council of Europe*, cit.*, 18).

giudicare, caso per caso, della loro "personalità". *In primis*, essi vengono raccolti e analizzati al fine di scoprire un *pattern* di gruppo a mezzo del già citato *KDD-process*[23]; il *pattern* di gruppo così individuato viene formalizzato nella generazione di un profilo di gruppo (*profile-generation*); tali profili di gruppo sono, a tutti gli effetti, "*new applicable information*", ovverosia nuovi dati; altri dati (*proxy*) saranno poi necessari per procedere all'*applicazione* dei profili di gruppo. Il profilo di gruppo, dunque, si configura come una formalizzazione di caratteristiche (non causalmente giustificate) riferite ad un insieme di persone variamente definito. L'applicazione del profilo di gruppo non viene considerato un trattamento di dati personali a meno che l'*attivatore del profilo* (la *proxy* attivatrice) non sia un dato personale esso stesso. Gli *input data,* infatti, nel corso del trattamento volto a generare il profilo di gruppo, vengono generalizzati, aggregati – dunque, anonimizzati – sì da generare un *profilo di gruppo* che non consente né la re-identificazione dei soggetti originali né l'identificazione dei nuovi soggetti cui esso andrà ad applicarsi. In altre parole, gli *identificatori* che li connotavano come "dati personali" vengono sostituiti da *identificatori* di gruppo privi del carattere della *personalità*, così privando il GDPR di ogni margine di applicazione.

Già da questa brevissima panoramica, è evidente che risolvere la questione sollevata in apertura – ovvero se il trattamento dei dati nel contesto della profilazione di gruppo sia ricompreso dalla portata applicativa del GDPR – non sarà un'operazione semplice: ogni passaggio della procedura poc'anzi descritta pone non pochi problemi – sicuramente legali ma anche etici – sul cammino verso la tutela delle persone fisiche coinvolte. Un individuo, pur non essendo «*identifiable*[24]», è comunque «*reachable*[25]» dagli effetti più rischiosi del trattamento. A questo punto, ci sarebbe da chiedersi quale sia il fattore di minaccia per i diritti e le libertà del soggetto in mancanza della sua identificazione. L'apparente assenza di rischio – sulla base del formalismo assunto per cui non v'è minaccia per il singolo se non vi sono singoli coinvolti – non deve trarre in inganno. La profilazione di gruppo, infatti, è potenzialmente in grado di ledere le persone fisiche coinvolte non meno di quella che avvenga ad livello individuale (cioè nel caso di identificazione del soggetto[26]). Tali rischi possono essere variamente categorizzati. Da una parte, possiamo individuare le *conseguenze non-materiali* della profilazione di gruppo, le quali ricadono per lo più sui singoli individui coinvolti. In questa categoria, rientrano la mancanza di trasparenza e, conseguentemente, il diniego del grado minimo di *informational self-determination*[27]*,*

[23] Cfr. *supra* nota 18.

[24] S. Barocas, H. Nissenbaum, *Big Data End's Run around Anonimity and Consent*, in J. Lane – V. S. Todden *et al., Privacy, Big Data, and the Public Good: Frameworks for engagement*, Cambridge, 2014, 45.

[25] *Ibid.*

[26] L. Taylor, *Safety in numbers? Group Privacy and Big Data Analytics in the Developing World*, in L. Taylor – L. Floridi *et. al.* (a cura di), *op. cit.*

[27] Ciò a causa dell'inapplicabilità dell'art. 5, par. 1, lett. a) e dell'art.13 [in particolare par. 2, lett. f)], art. 14 [in particolare par. 2, lett. g)] e art. 15 [in particolare par. 1, lett. h)] Reg. EU 679/2016. Sul punto, si veda: M. Hildebrandt, *The Dawn*

il cd. rischio di de-individualizzazione[28] e, più in generale, il mancato raggiungimento di livelli accettabili di privacy dei soggetti coinvolti, sia nel senso di "controllo" che di "inaccessibilità"[29]. In modalità differenti, invece, si atteggiano le *conseguenze materiali* della profilazione di gruppo. Queste possono essere a loro volta divise tra *conseguenze materiali ad un livello prettamente individuale* (ossia il fenomeno dei falsi applicativi e l'implementazione di decisioni automatizzate per mezzo dei profile di gruppo senza che il soggetto possa accedere – in virtù della sua non identificabilità – alle salvaguardie dell'art. 22[30] e il rischi di discriminazione) e *conseguenze materiali a livello collettivo/sociale* (cioè una discriminazione su larga scale e, conseguentemente, una crescente segmentazione della società).

In questa sede, intendiamo concentrarci su tre dei problemi evidenziati dalla tassonomia qui accennata (le decisioni automatizzate e la non applicazione dell'art. 22, il caso dei falsi applicativi, i rischi di discriminazione e segmentazione della società), tentando di capire, da un lato, in che modo l'applicazione della disciplina in materia di protezione di dati personali potrebbe giovare a tali problematiche e, d'altro canto, come limare, pur nella sua impossibilità, gli spigoli più dannosi delle loro conseguenze.

2.1. Le decisioni automatizzate a livello di gruppo

Ad oggi, i processi decisionali «basati unicamente sul trattamento automatizzato di dati[31]» *si svolgono sempre* più ad un livello "di gruppo" e sempre meno sulla base della considerazione individuale del singolo soggetto. Come già accennato, "predizioni" e "decisioni" possono essere implementate su un gruppo non meno efficacemente che su un singolo individuo[32]: è ben possibile che un soggetto sia sottoposto a profilazione e che, su questa base, vengano prese decisioni automatizzate che lo riguardano, senza che questo si traduca nella sua identificazione personale[33]: il solo fatto che la persona venga sottoposta a decisioni esterne – senza che le sia garantito un minimo grado di consapevolezza dell'av-

of a Critical Transparency Right for the Profiling Era, in *Selected Works*, 2012 Disponible su: <https://works.bepress.com/mireille_hildebrandt/40/>; A. Rouvroy – Y. Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy* in S. Gutwirth *et al.* (a cura di), *Reinventing Data Protection?* Springer, 2009.

[28] A.H. Vedder, *KDD: The challenge to individualism*, in *Ethics and Information Technology*, 1999, 275 e ss.

[29] B. Rössler, *The Value of Privacy*, Polity Press, 2005.

[30] Art. 22, Reg. EU 679/2016: diritto di non essere soggetti ad una decisione del tutto automatizzata, diritto di ottenere l'intervento umano, diritto di esprimere il proprio punto di vista, diritto di contestare la decisione.

[31] *Ivi*.

[32] B. Mittelstadt, *From Individual to Group Privacy in Big Data Analytics*, in *Philosophy&Technology*, 2017, 6 e ss.

[33] Come efficacemente si legge in L.Taylor, *Safety in numbers? Group Privacy and Big Data Analytics in the Developing World*, in L.Taylor, L.Floridi et. al (a cura di), *op. cit.*, p. 14: «We may be profiled in actionable ways without being personally identified»; o, ancora: «in an era […] where analytics are being developed to operate at as broad a scale as possible, the individual is […] incidental to the analysis» (L. Taylor – L. Floridi – B. van der Sloot, *Introduction: A New Perspective on Privacy*, in L. Taylor – L. Floridi *et al.* (a cura di), *Group Privacy: New Challenges of Data Technologies*, Springer, 2017, p. 2.

venuta operazione e senza assicurarle la possibilità di contestare i risultati del processo – è una violazione della sua personalità a prescindere dalla natura dei mezzi (*personali* o meno) utilizzati per raggiungere detto effetto[34].

Sic rebus stantibus, la necessità di estendere la portata applicativa del GDPR anche a tali situazioni è quanto mai urgente[35]. Se, com'è vero, i processi decisionali che avvengono a livello individuale e quelli che, invece, hanno luogo su un livello prettamente collettivo hanno effetti, sugli individui coinvolti, sostanzialmente equivalenti, allora dovremmo, sulla base di questa similarità, equiparare anche il trattamento giuridico di cui godono le due forme di profilazione. Poco senso avrebbe l'opposta opzione: regolare situazioni *de facto* analoghe in modalità radicalmente differenti. Eppure, *in claris non fit interpretatio*: l'assenza del requisito della "*singolarità*" e della "*distinguibilità*" obbliga il giurista all'opposta conclusione. La formulazione dell'articolo, infatti, riferisce esplicitamente il diritto ad attivare le tutele offerte all'«*interessato al trattamento*[36]». Questo, congiuntamente con quanto prima accennato circa la necessità della "distinguibilità" e della "singolarità" del soggetto a cui sono riferiti i dati, esclude l'applicabilità dell'articolo ai casi in cui la *decisione* venga *azionata* sulla base di *identity-proxies* condivise da una molteplicità indistinta di persone. Pur non potendo evitare, pena il mancato rispetto del dato testuale, tale *interpretatio ad excludendum*, non possiamo però esimerci dal notare che essa è intimamente contraria alla *ratio* dell'articolo stesso. D'altronde, se il *focus* dell'art. 22 fosse la protezione *per sé* dei dati personali, poco senso avrebbe la limitazione della sua portata applicativa sulla base dell'entità delle conseguenze che tale trattamento *de facto* produce[37]. L'art. 22, infatti deve essere interpretato come uno strumento per mitigare sul piano pratico i potenziali effetti negativi del trattamento di dati, a prescindere dalla *personalità* dei mezzi con cui questi effetti vengono prodotti. In altre parole, l'obiettivo di *policy* che ispira l'articolo è quello di porre un argine alle *conseguenze* dannose del trattamento – regolando le situazioni concrete che ne conseguono – e non impedire *a priori* il suo svolgersi. Sotto tale luce, la limitazione della portata applicativa dell'art. 22 al solo interessato al trattamento appare

[34] L. Floridi, *four challenges for a theory of informational privacy*, in *Ethics and Information Technology*, 2006, 112.

[35] L'urgenza nasce non solo dalla gravità dei rischi che tale pratica presenta, ma anche dall'estensione del suo utilizzo: la profilazione di gruppo presenta notevoli vantaggi per chi di essa fa la base del suo business model: è una nuova modalità di selezione dei target sicuramente più «cost-efficient» della profilazione individuale in quanto permette di concentrare l'attenzione su un gruppo di individui *clusterizzati* sulla base di determinate proprietà piuttosto che su un singolo *token,* così evitando le problematicità che derivano dal gestire enormi quantità di informazioni [L. Taylor – L. Floridi – B. van der Sloot, *Introduction: A New Perspective on Privacy*, in L. Taylor – L. Floridi *et al.* (a cura di), *op. cit.*, 10].

[36] Art. 22, Reg. EU 679/2016, *cit.*

[37] Le salvaguardie dell'art. 22 (*Ivi*) infatti, sono limitate ai casi in cui la decisione abbia sull'interessato al trattamento «effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

incoerente con lo spirito che anima articolo: in quanto tale trattamento va a spiegare i propri effetti anche (e prevalentemente[38]) su soggetti non identificati e non identificabili[39]. A sostegno di un tale argomentare, si guardi anche al raffronto con l'articolo corrispondente della precedente direttiva in materia di protezione dei dati personali[40] e, soprattutto, alla precedente versione dell'articolo nella proposta di Regolamento[41]. L'art. 15 della Direttiva, infatti, eleggeva ad elemento dirimente per l'applicazione dell'articolo non la *personalità* dei dati trattati, bensì il fatto se le conseguenze del trattamento presentassero o meno determinate caratteristiche[42]. Il titolare degli strumenti di tutala offerti dall'art. 15 della Direttiva, infatti, era «qualsiasi persona[43]» e non – com'è invece nell'attuale art. 22 del GDPR – "l'interessato al trattamento", che, come poc'anzi detto, deve necessariamente essere identificabile, *id est* singolarmente distinguibile). Con l'obiettivo di non diminuire il grado di protezione offerto dalla Direttiva, anche la Proposta di Regolamento, all'art. 20, descriveva il titolare del diritto in questione come «every natural person[44]». A quanto sembra, la sostituzione di tale dicitura – capace di eliminare l'ostacolo testuale con cui l'interprete attualmente si scontra nell'estendere l'applicazione dell'articolo – con l'attuale formula è il frutto di un «editorial or technical amendment or clarification[45]», non figlia, dunque, della volontà espressa di ridurre la portata applicativa dell'articolo in questione sulla base di una valutazione consapevole delle circostanze e dei rischi del caso: pur a fronte di un cambiamento di forma esteriore, le ragioni di politica legislativa sottese all'articolo non sembrano mutate. Tuttavia, il dato testuale è inequivocabile: al giurista non resta che prendere atto di tali *ombre* e unirsi all'accorata dottrina che, dopo aver fatto notare che le «decision[i]» di cui all'art. 22 possono esser prese ad un livello individuale non meno efficacemente che ad un livello di gruppo[46], si vede obbligata ad esclamare che «there is no safety in numbers[47]» e che, anzi, la mancata identificazione del soggetto, lungi

[38] Cfr. *supra*, nota 35.

[39] Anzi, l'applicazione dell'art. 22 si rende ancora più necessaria nel contesto della profilazione di gruppo in virtù dei particolari rischi (applicazioni false o discriminatorie, per cui si veda *ultra*) che tale pratica pone. B. Schermer, *Risks of Profiling and the Limits of Data Protection Law*, in B. Custers – T. Calders *et al.* (a cura di), *op. cit.*, 140.

[40] Art. 15, Dir. 95/46/EC, 24 ottobre 1995, GU L 281.

[41] Art. 20, Commissione Europea, *Proposta per un Regolamento del Parlamento Europeo e del Consiglio relativo alla protezione degli individui con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento Generale sulla Protezione dei Dati)*, 25 gennaio 2012.

[42] In particolare, se la profilazione si traduce in una «decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti» e questa è fondata «esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità» (Art. 15, Dir. 95/46/EC, cit.), allora le particolari cautele approntate dall'art. 15 della direttiva e, relativamente al rispetto del principio di trasparenza, dall'art. 12, par. 1 troveranno margini applicativi.

[43] *Ibid.*

[44] Cons. 58 e Art. 20, Commissione EU, Proposta per un Regolamento, cit.

[45] Informazione disponibile su: <https://lobbyplag.eu/governments/gdpr>.

[46] B. Mittelstadt, *op. cit.*, 3 e 9.

[47] L. Taylor, *Safety in Numbers?*, cit.

da essere una barriera protettiva dai pericoli cui il soggetto è esposto, non è nient'altro che un nuovo *vulnus* ai meccanismi di tutela dello stesso, in quanto fattore impeditivo dell'applicabilità della tutela di cui è possibile beneficiare nei casi in cui il requisito della *personalità dei dati* sia presente.
Tornando alla domanda da cui siamo partiti, dunque, non possiamo esimerci dal notare, almeno nell'ambito qui esposto, un'incongruenza tra l'obiettivo dichiarato – cioè, nel caso specifico dell'art. 22, la protezione dagli effetti negativi del trattamento – e gli strumenti preposti al suo raggiungimento, il che si traduce, in accordo alla nota metodologica con cui si è aperto questo contributo, in un certo grado di inefficacia del Regolamento.

2.2. Le applicazioni false o discriminatorie dei profili di gruppo

Come già accennato, la profilazione di gruppo può portare a conseguenze *ingiuste*, sia sul singolo individuo coinvolto dalla sua applicazione (applicazioni errate, cd. falsi applicativi, o discriminatorie) sia, più in generale, sulla collettività (discriminazione su larga scala e conseguente segmentazione della società)[48]. Tali ultime problematiche collettive, già gravi di per sé, sono rese ancora più insopportabili dalla mancata applicazione di quegli articoli che consentono al "soggetto leso" di essere specificamente informato delle caratteristiche della decisione presa esclusivamente sulla base del profilo di gruppo e di contestare gli effetti dell'applicazione del profilo[49].
Accingendoci ad un'analisi più specifica e dettagliata degli elementi potenzialmente dannosi precedentemente accennati, varie sono le considerazioni da fare. In prima istanza, per quanto concerne il caso dei cd. falsi applicativi, parliamo di *falso applicativo* quando ad un soggetto è erroneamente associato un profilo che non risponde alle sue reali caratteristiche (falso positivo) o quando è tralasciato dall'applicazione di un profilo che invece gli sarebbe di fatto calzante[50]. Un simile rischio è l'inevitabile conseguenza della applicazione di *profili di gruppo non distributivi*[51]. Il pericolo di sfociare in false applicazioni, infatti, è intrinseco al funzionamento stesso dei profili di gruppo non distributivi[52]. Questi,

[48] B. Custers – T. Calders, et al. (a cura di), *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases*, Springer, 2013.

[49] Alla già discussa inapplicabilità dell'art. 22, Reg. EU 679/2016, cit. (*supra,* sez. 2.1) segue, infatti, l'inapplicabilità dell'art. 13, par. 2, lett. f), art. 14, par. 2, lett. g e art. 15, par. 1, lett. h), Reg. EU 679/2016, cit.

[50] K. Wiedemann, *Automated Processing of Personal Data for the Evaluation of Personality Traits: Legal and Ethical Issues*, in Max Planck Institute, 2018, 11. Disponibile su: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102933>.

[51] B. Custers, *Data Dilemmas, cit*., p. 13: «Group profiles differ from individuals with regard to the fact that the properties in the profile may be valid for the group and for individuals as members of that group, though not for those individuals as such. If this is the case, this is referred to as non-distributivity or non-distributive properties. […] When properties are valid for each individual member of a group as an individual, this is referred to as distributivity or distributive properties». In sostanza, per quel che più rileva in questa sede, i profili di gruppo distributivi si applicano singolarmente agli individui anche se sulla base di proxy che difettano del requisito dell'identificabilità, i profili di gruppo non distributivi si applicano, invece, a raggruppamenti di persone in modo del tutto indistinto.

[52] Si guardi, ad esempio alla definizione di profilazione fornita da Council of Europe, *Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD),* 11 gennaio 2008, T-

infatti, applicandosi all'intero gruppo piuttosto che ai singoli membri su base individuale, presentano una componente strutturale e ineliminabile di errori applicativi, i quali rientrano nella *fisiologia* – e non nella *patologia* – delle peculiarità tecniche di tale pratica. Il funzionamento della profilazione di gruppo, difatti, si basa esclusivamente su strumenti statistici (medie, mediane, probabilità, devianze, …) che, in quanto tali, presentano un certo margine di errore ineliminabile[53]. Nelle parole di autorevole dottrina, la profilazione di gruppo può facilmente sfociare in un trattamento fortemente differenziato sulla base di caratteristiche «irrilevanti[54]», cosicché l'applicazione del profilo risulterà, nei fatti, "ingiusta" o scorretta per alcuni – ma non per un numero sufficiente da portare all'inefficienza della procedura – degli individui da questa toccati[55]. In sostanza, per quel che più rileva in questa sede, poiché i profili di gruppo non distributivi si applicano a raggruppamenti di persone in modo del tutto indistinto, il profilo di gruppo, anche se valido per gli individui *in quanto membri* di quel gruppo, potrebbe essere non calzante per gli individui in sé e per sé considerati. Poiché il profilo, però, riguarda il *gruppo* nella sua totalità e non i suoi *membri* in quanto singoli, ai casi *fisiologici* di falsa applicazione non consegue una perdita di *efficienza* della procedura nella sua totalità.

In secondo luogo, dobbiamo focalizzarci sulle potenziali conseguenze discriminatorie dell'applicazione del profilo di gruppo. Come è stato detto, anche se l'algoritmo che genera e applica il profilo non utilizza dati sensibili e potenzialmente discriminatori, *«discrimination is part and parcel of profiling*[56]*»*. Infatti, non solo è ben possibile che l'algoritmo presenti, nel suo funzionamento, dei *bias* discriminatori[57], ma, anche a voler tacere di tali rischi "tecnici", la possibilità di risultati potenzialmente discriminatori sussisterebbe comunque[58]. Le cd. "*shared identity proxies*" che associano il profilo di gruppo all'indi-

PD(2008)01, p. 3 e ripresa anche da European Union Agency for Fundamental Rights (FRA), *Preventing Unlawful profiling today and in the future: a guide*, 2018, p. 15: «Profiling includes data mining whereby individuals are categorised on the basis of some of their characteristics in order to infer, with a certain margin of error, others that are not observable».

[53] A.H. Vedder, *op. cit.*, 1999, 277.

[54] T. Zarsky, *The trouble with algorithmic decisions an analytic road map to examine efficiency and fairness in automated and opaque decision making*, in *Science, Technology & Human Values*, 2016, 118-132.

[55] *Ibid.*, Sul punto si veda anche M. Hildebrandt, *Profiling and AmI*, in K. Rannenberg – D. Denis Royer *et al.*, *The Future of Identity in the Information Society: Challenges and Opportunities*, Springer, 2009, 278 and ss.

[56] B. Schermer, *Risks of Profiling and the Limits of Data Protection Law*, in B. Custers – T. Calders *et al.* (a cura di), *op. cit.*, 138.

[57] C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown book, 2016; V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Press, 2017; S. Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism,* New York University Press, 2018.

[58] B. Schermer, *op. cit.,* p. 138: «even without a prior desire to judge people on the basis of particular characteristics, there is the risk of inadvertently discriminating against particular groups or individuals» (*Ibid.*). Sulle difficoltà tecniche che si incontrano nel tentativo di evitare le conseguenze discriminatorie della profilazione (nonché di scoprire il potenziale discriminatorio insito nel trattamento) si veda D. Pedreschi – S. Ruggieri *et al.*, *The Discovery of Discrimination*, in B. Custers – T. Calders *et al.* (a cura di), *op. cit.*, 91 e ss. Tale rischio è riconosciuto anche da European Union Agency for Fundamental Rights (FRA), *op. cit.*, 16, che specifica che «in developing algorithmic profiling, bias may be introduced at each step of the processing».

viduo, infatti, vanno spesso a coincidere con *informazioni sensibili*[59] (ad esempio, età, provenienza, nazionalità, abitudini sessuali, condizioni di salute, …). Non solo, ma anche quando le *proxy* di attivazione del profilo appaiono assolutamente *neutre* ai sensi della normativa antidiscriminazione, è ben probabile che esse si correlino con caratteristiche potenzialmente discriminatorie, così contribuendo a perpetrare inaccettabili forme di segregazione di alcuni gruppi e segmentazione della società[60]. Si pensi, ad esempio, al fatto che un dato "neutro", quale può essere lo *zip code,* tende, in alcuni casi, a correlare con l'origine etnica e, dunque, con le credenze religiose o l'orientamento politico del soggetto. La "neutralità" della *proxy* di attivazione del profilo, infatti, non è sufficiente a garantire che i risultati dell'applicazione del profilo, anche se non discriminatori nell'intento, lo siano su un piano fattuale[61], con ciò aumentando sensibilmente la probabilità che l'utilizzo su larga scala di tali *"sensitive-features-correlated" group profiles* porti a conseguenze discriminatorie[62] per il singolo e per la società tutta[63].

3. I benefici (impossibili) dell'applicazione del GDPR

La necessità di estendere alcune delle tutele che il GDPR offre anche al caso dell'applicazione di profili di gruppo è evidente. I benefici che deriverebbero dall'applicazione del Regolamento, infatti, sono evidenti. Anzitutto, gli individui coinvolti da decisioni automatizzate sulla base di profili di gruppo, si vedrebbero riconosciuto un grado minimo di trasparenza e di tutela pratica nei confronti degli effetti negativi delle decisioni automa-

[59] *Melius*, «categorie particolari di dati personali» *ex* art. 9, Reg. EU 679/2016, cit.

[60] Secondo D. Pedreschi – S. Ruggieri *et al.*, *op. cit.*, 92: «apparently neutral practices that take into account personal attributes correlated with indicators of race, gender, and other protected grounds and that result in discriminatory effects on such protected groups». Sul tema si guardi anche: T.Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Rev.*, 2017, 1112 and ss. di cui in particolare 1113; L. Moerel, *op. cit.*; P. Ohm, *Sensitive information*, *op. cit.*

[61] Tale rischio si colora di concretezza e attualità ancora maggiori se si considera la ridottissima «computational distance» (G. Malgieri – G. Comandè, *Sensitive-by-distance, op. cit.*, 11).

[62] Per una carrellata di esempi in cui l'attività di profilazione sulla base di informazioni *latu sensu* si veda: J. Angwin *et al.*, *Machine bias: there's software used across the country to predict future criminals. And it's biased against blacks*, in *ProPublica*, 2016, disponibile su: <https://www.ProPublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>; J. Angwin – N. Scheiber *et al.*, *Dozens of companies are using Facebook to exclude older workers from job ads*, in *ProPublica*, 2017, disponibile su: <https://www.propublica.org/article/facebook-ads-age-discrimination-targeting>; J. Angwin – A. Tobin *et al.*, *Faceboook (still) letting housing advertisers exclude users by race*, in *ProPublica*, 2017, Disponibile su: <https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin>; L. Sweeney, *Discrimination in Online Ad Delivery: Google ads, black names and white names, racial discrimination, and click advertising,* in *ACMqueue,* 2013, 11, 3; J. Angwin – S. Mattu et al., *The Tiger Mom Tax: Asians are nearly twice as likely to get a higher price from Princenton Review*, in *ProPublica*, 2015, disponibile su: <https://www.ProPublica.org/article/asians-nearly-twice-as-likely- to-get-higher-price-from-princeton-review>; J. Larson – S. Mattu, *Unintended consequences of Geographic targeting*, in *Technology Science*, 2015, disponibile su: <https://techscience.org/a/2015090103/>.

[63] Per un inquadramento sistematico delle modalità con cui gli effetti discriminatori possono venire alla luce, si veda Council of Europe, *Discrimination, artificial intelligence, and algorithmic decision-making*: study by F.Z. Borgesius, 2018, 10-17.

tizzate prese sulla base dei profili di gruppo[64]. In secondo luogo, gli individui danneggiati dalle false applicazioni del profilo di gruppo poterebbero trarre benefici dal principio di «correttezza[65]» e «esattezza[66]» del trattamento, interpretati in connessione con il cons. 71[67]. Infine, le conseguenze potenzialmente discriminatorie del trattamento potrebbero essere mitigate dall'applicazione del principio di «correttezza[68]» e «liceità[69]», ancora una volta in connessione con i considerando 71[70] e 75[71].

Ovviamente, a fronte di un dato testuale netto e preciso come quello dell'art. 4(1)[72], tali forme di protezione non sono applicabili. Eppure, il calibro delle problematicità qui emerse e il tenore dei diritti messi a rischio da una tale situazione, impone al giurista una riflessione ulteriore sulla possibilità di ricondurre questo panorama ad una forma di regolazione alternativa, basata su plessi normativi che non facciano della *personalità del dato* il punto focale della loro applicabilità. Se, come è vero, il problema dell'inapplicabilità del GDPR alla profilazione di gruppo risiede nella mancata *singolarità* e nella *non-distinguibilità* degli individui coinvolti, allora, a rigor di logica, l'elaborazione di un regime di tutela non potrà che far perno sulla prima fase della profilazione di gruppo, ovverosia *prima* che l'aggregazione e la definitiva generalizzazione e anonimizzazione dei dati sbarrino la via all'applicabilità del Regolamento. Solo in questo stadio, quando cioè i dati non sono ancora stati "scollegati" dall'identificatore che consente di riferirli ad un soggetto *singolo* e *distinguibile*, il Regolamento avrà un qualche margine di applicazione. Sarà a questo momento (la racconta o l'ottenimento dei dati per altre vie), dunque, che il giurista dovrà guardare nella speranza di elaborare una qualche forma di tutela per i profili di rischio fino ad ora evidenziati. È fondamentale, però, un *caveat* preliminare: la "collocazione" logica e temporale dei meccanismi protettivi che ora analizzeremo in una dimensione che precede – logicamente e cronologicamente – il momento realmente "dannoso" del trattamento (ossia l'applicazione del profilo), non si traduce nella formalizzazione di un sistema in grado di tutelare solo i soggetti – per usare il lessico del Regolamento – identificati dai

[64] Cfr. *supra*, sez. 2.1.

[65] Art 5, par. 1, lett. a), Reg. EU 679/2016, cit.

[66] *Ivi,* art 5, par. 1, lett. d) «I dati personali sono […] esatti […]; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti».

[67] *Ivi*, cons. 71, che afferma che «al fine di garantire un trattamento corretto […] è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori».

[68] *Ivi,* art 5, par. 1, lett. a).

[69] *Ibid*.

[70] *Ivi,* cons. 71, che afferma che i dati devono essere trattati con una «modalità che […] impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche […] ovvero che comportano misure aventi tali effetti».

[71] *Ivi,* cons. 75, che afferma che il «se il trattamento può comportare discriminazioni» il titolare del trattamento deve prestare particolare attenzione alla valutazione dei rischi».

[72] *Ivi,* Art. 4 (1).

dati[73] personali. Regolando il "prima" per influenzare il "poi", anche i soggetti (non singolarmente distinguibili) coinvolti dalle conseguenze dannose della profilazione riceveranno una qualche forma di tutela.

4. La normativa antidiscriminazione: un'alternativa da scartare

Converrà preliminarmente dar conto di come si è giunti alla conclusione che il miglior modo per incidere sulle problematiche esposte nei paragrafi precedenti sia l'applicazione della disciplina in materia di trattamento dei dati personali. Autorevole dottrina, infatti, partendo dalla conclamata incapacità del GDPR di regolare le conseguenze *non personali* della profilazione di gruppo, ha tentato di porre un argine ai segnalati fenomeni guardandoli come fatti a sé stanti, *indipendenti* dalla modalità con cui vengono posti in essere (profilazione sulla base di dati). In altre parole, a prescindere dai mezzi utilizzati (ovverosia *dati*) per ottenere gli effetti di cui sopra, la dottrina ha indagato plessi normativi differenti nella speranza di poter trovare una qualche forma di protezione per i soggetti toccati dalle derive *patologiche* degli effetti *fisiologici* della profilazione di gruppo[74]. Poiché, infatti, il fulcro della questione si sposta, dalla regolazione del trattamento dei dati *per se*, sugli effetti concreti e materiali dello stesso, sarà sicuramente possibile, qualora se ne integrassero le condizioni di applicazione, optare per sistemi normativi diversi dal Regolamento *ad hoc*. Come già accennato, su questa base, parte della dottrina[75], ha soppesato la possibilità intervenire sui fatti in questione a partire da plessi normativi diversi dalla normativa in materia di protezione dei dati personali, nella speranza di aggirare le problematicità[76] cui

[73] *Ibid.*

[74] Cfr. *supra*, sez. 2.2.

[75] A titolo esemplificativo: B. Custers – T. Calders *et al.* (a cura di), *op. cit.*, di cui si veda, in particolare, B. Schermer, *op. cit.*, 137 e ss e R.Gellert – K. de Vries *et al.*, *A Comparative Analysis of Anti-Discrimination and Data Protection Legislations,* p. 82 ; L. Taylor – L. Floridi *et. al.* (a cura di), *op. cit.*, di cui si veda in particolare A. Mantelero, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, 139 e ss.; W. Schreurs – M. Hildebrandt *et al.*, '*Cogitas, Ergo Sum*'. *The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector*, in M. Hildebrandt – S.Gutwirth, *Profiling the European Citizen: Cross-Disciplinary Perspectives,* Springer, 2008.

[76] Optando per il plesso normativo della *data-protection law*, il meccanismo di protezione non potrà che inerire alla fase di raccolta dei dati personali, cioè prima che l'aggregazione e l'anonimizzazione dei dati inibiscano ogni possibilità di applicare il Regolamento. Tuttavia, il momento della raccolta di dati, il più delle volte, non è il *locus* dove meglio si evidenziano le derive della profilazione di gruppo poc'anzi menzionate. Ancora una volta, impedendo l'applicazione delle tutele del Regolamento alle fasi successive della profilazione di gruppo, la "trappola della non personalità" priva il Regolamento di effettività.

l'applicazione GDPR va incontro. In particolare, gli sforzi si sono concentrati sull'obiettivo di limitare le conseguenze discriminatorie dell'applicazione dei profili di gruppo[77].
Vista la caratura del problema, non meraviglia se la scelta è immediatamente ricaduta sulla normativa antidiscriminazione[78]. Eppure, ad una più attenta analisi, è la stessa natura della profilazione di gruppo a remare contro tale soluzione: innanzitutto, gli effetti discriminatori della profilazione di gruppo, in quanto "indiretti"[79], potrebbero essere facilmente considerati *giustificati*[80] da un obiettivo legittimo[81] ma, anche a tacere di questo, bisogna riconoscere che, in virtù delle peculiarità strutturali del *KDD-process* e della "nuova epistemologia" da esso fondata[82], la volontà di applicare la normativa antidiscriminazione al caso di specie non può che risolversi in una macroscopica forzatura. Il metodo "tradizionale[83]" di categorizzazione della società, infatti, muove a partire da classi *già* esistenti, che fungono da presupposti logici e cronologici della procedura, la quale consiste, prevalentemente, nell'individuazione delle caratteristiche dirimenti che converrà utilizzare al fine di collocare i soggetti nella categoria che più si addice loro; un processo, dunque, deduttivo che si svolge a partire dalla teorizzazione dell'esistenza di una classe e prosegue con la valutazione degli individui sulla base di caratteristiche individuate come *costituti-*

---

[77] B. Goodman, *Discrimination, data sanitisation and auditing in the European Union's General Data Protection Regulation*, in *EDPL*, 2, 2016; P. Hacker, *Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law*, in *Common Market Law Rev.*, 4, 2018, 1143-1185; si veda anche European Monitoring Centre on Racism and Xenophobia, *Perceptions of discrimination and islamophobia: voices from members of Muslim communities in the European Union*, 2006, 54.

[78] Dir. 2000/43/EC; Dir. 2000/78/EC; Dir. 2002/73/EC; Dir. 2006/54/EC; Art. 21 della Carta dei diritti fondamentali e il Protocollo 12; Art. 14 della Convenzione Europea dei Diritti dell'Uomo. In particolare, si segnala la differenza tra discriminazione diretta e indiretta. *Ex* art. 2, Dir. 2000/43/EC: si ha discriminazione indiretta quando la *neutralità* di un criterio, di una pratica o di una regola si traduce in uno svantaggio per le persone che presentano un certo attributo sensibile; La pratica indirettamente discriminatoria è consentita se *giustificata* da un obiettivo legittimo perseguito con mezzi idonei e proporzionali. Sul punto si veda, ad esempio C. Tobler, *Limits and potential of the concept of indirect discrimination*, Eu Network of Legal Experts in Anti-Discrimination. Disponibile su: <http://www.migpolgroup.com>. Per un quadro più generale della normativa antidiscriminazione e la giurisprudenza europea in materia si veda European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European non-discrimination law*, 2018.

[79] European Union Agency for Fundamental Rights (FRA), *Preventing Unlawful profiling today and in the future: a guide*, 2018, 24-26.

[80] *Ivi*, p. 22, in cui si afferma che l'attività di profilazione può essere considerata "*unlawful*" solo nel caso in cui il trattamento differenziato a cui sono sottoposti gli individui risulti del tutto «unjustified».

[81] Così escludendo dalla portata applicativa della legislazione in tema di antidiscriminazione la maggior parte delle situazioni che si presentano nel caso della profilazione di gruppo. A tal proposito, si veda W. Schreurs – M. Hildebrandt *et al.*, *op. cit.*, 260, in cui si afferma che le differenziazioni tra persone fisiche, effetto (e obiettivo) della profilazione di gruppo, sono basate su una «objective and reasonable justification». Non sono mancati, in tal senso, pareri da parte delle Istituzioni: «profiling may thus provide benefits for users, the economy and society at large» (Comitato dei Ministri del Consiglio d'Europa, *cit.*, p. 1) e, dunque essere nell'interesse legittimo «of both the person who uses it and the person to whom it is applied, […] by [...] adapting offers to meet demand by the provision of better services» o, più in generale, migliorando la «consumers' and users' experience» (Council of Europe, *cit.*, 18).

[82] Cfr. *supra*, nota 20.

[83] Il paragone con le tecniche di segmentazione della società e categorizzazione degli individui cui siamo abituati è d'obbligo: secondo Council of Europe, *cit.*, 28 la profilazione di gruppo, infatti, può esservi – sicuramente nelle finalità, parzialmente negli effetti – del tutto assimilata. I profili, infatti, hanno le stesse fattezze e svolgono lo stesso ruolo delle categorie socialmente determinate e percepite.

ve della classe stessa e *sintomatiche* dell'appartenenza di un soggetto a detta classe. La categorizzazione degli individui tramite profilazione di gruppo nel contesto dei *Big Data*, al contrario, si imposta come un meccanismo prettamente *induttivo*, che, senza ricorrere a categorie pre-esistenti[84], individua le classi e i tratti costitutivi delle stesse sulla base di correlazioni e *pattern* scoperti nella fase di *data-mining*. Le categorie individuate nella fase di *Big Data Analytics* sono, dunque, «*socially a-significant*[85]», per non dire «*fuzzy*[86]*»: del tutto prive di ogni caratura morale e indipendenti da ogni stereotipo o pregiudizio, esse stupiscono per la loro imprevedibilità,* consentendo una segmentazione della società[87] che fa della sua "neutralità" ideologica, politica, culturale ed estetica un arnese affilato e preciso, capace di regalare ai profili di gruppo così generati e applicati una nuova e inaspettata accuratezza[88]. Addirittura, autorevole dottrina[89], volgendo lo sguardo agli aspetti più tecnici della profilazione di gruppo, afferma che, paradossalmente, l'applicazione dei profili di gruppo – e la conseguente segmentazione della società sulla base di classi di riferimento così elaborate nel contesto della *Big Data Analytics* – possa essere una vera e propria arma contro la discriminazione sulla base di caratteristiche sensibili. Il *data mining* che porta all'elaborazione dei profili di gruppo fa della sua «cecità[90]» e "*indifferenza*" alla predeterminazione sociale delle categorie e, contestualmente, della sua "permeabilità" ai soli dati (di fatto) delle correlazioni registrate nel *database* un utile strumento per garantire, ad un sol tempo, una maggiore efficienza *economica*[91] della procedura e una valutazione assolutamente imparziale delle persone coinvolte da questa: tutti sono sottoposti agli stessi criteri di giudizio, agli stessi parametri, alle stesse "unità di misura"[92]. È dunque evidente

[84] A. Mantelero, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, 145, in L. Taylor – L. Floridi *et al.* (a cura di), *op. cit.*, 139 and ss.

[85] L. Kammourieh – T. Baar *et al.*, *Group Privacy in the Age of Big Data,* in L. Taylor – L. Floridi *et al.* (a cura di), *op. cit.*, 41.

[86] L. Taylor, *Safety in Numbers*, *cit.*, 15.

[87] Tali gruppi – *melius*, raggruppamenti – non sono self-constitued» ma «algorithmically-grouped»: si presentano come «new forms of population segments, dispersed throughout society and only connected by some attributes they have in common» (B.Custers – T. Calders *et al.*, *The way forward*, in B.Custers – T. Calders *et al.* (a cura di), *op. cit.*, 342), con l'estrema conseguenza che «such groups will lack political force to defend their interests» (*Ibid.*).

[88] *Ibid.* ma anche S. Thatcher, *reply* to W. Schreurs – M. Hildebrandt *et al.*, *op. cit.*, 264.

[89] T. Zarsky, *Governmental Data Mining and its Alternatives*, in *Penn State Law Rev.*, 2011, 285-330.

[90] Council of Europe*, cit.*, 29.

[91] A tal proposito, in S. Whatcher, *reply, cit.*, 268-269 si sostiene che «discrimination is fundamental to successful commerce» e che «the commercial setting […] negates its exploitative nature». Conseguentemente, «economic imperatives will militate against [the use of antidiscrimination law] as a defence to the application of group profiles» (*Ibid.*).

[92] Addirittura, alcune voci (B. Custers, T. Calders, et al., *The way forward*, in B.Custers – T. Calders *et al.* (a cura di), *op. cit.*, 353 e ss.), a loro stesso dire «unnecessarily paranoid» (*Ibid.*) si sono levate contro il possibile utilizzo della *antidiscrimination law*: dopo aver definito la volontà di regolare le pratiche di *data-mining* una «irrational, Luddite-like fear» affermano che «the seeming intuition that data mining leads to unacceptable discrimination is merely a manipulation of the powerful trying to influence the weak. While automated practices might finally lead to equal treatment, they might compromise the elite's dominance and subject them to the same level as scrutiny as everyone else (something they are not used to)». Similmente, T. Zarsky, *Governmental Data Mining*, cit., 323 e ss.

che il principio di non discriminazione non è lo strumento idoneo ad elaborare una forma di regolazione e limitazione delle conseguenze sociali della profilazione di gruppo[93]. Più che di discriminazione, infatti, si dovrebbe parlare di *differenziazione* (o di riconoscimento di una differenza), che, a seconda della presenza o meno delle correlazioni positive con fattori sensibili ai sensi della normativa antidiscriminazione, può tradursi, al più, in *segmentazione sociale* o discriminazione *indiretta* ma *giustificata*.

5. La "trappola della non personalità"

È il momento, ora, di fare un passo indietro e abbracciare il problema da più ampie prospettive. Aver scartato l'ipotesi di regolare le conseguenze della profilazione di gruppo ricorrendo a strumenti normativi altri rispetto alla *data-protection law* non vuol dire, però, che si debba persistere nell'infruttuoso tentativo di allargare la nozione di personalità al fine di ricomprendervi anche i problemi che in essa, *stricto iure,* non troverebbero spazio. Guardando ai profili tecnici della profilazione di gruppo[94], infatti, è ben possibile individuare un momento della procedura – quello precedente alla generazione del profilo di gruppo – in cui i dati trattati, non ancora aggregati (e de-personalizzati) nella generazione del profilo, possono essere qualificati come *personali ex* art. 4(1)[95], così da consentire l'applicabilità delle previsioni del GDPR. Su questa base, la proposta con cui vogliamo terminare la nostra analisi consiste nel mitigare le conseguenze dannose della profilazione di gruppo tramite una «valutazione d'impatto sulla protezione dei dati[96]» (*DPIA*) prima della loro *de-personalizzazione*, quando il GDPR gode ancora di un qualche margine applicativo.

Anche se l'applicabilità delle previsioni in materia di DPIA non può essere estesa alle fasi del trattamento che, nei fatti, sono in grado di ledere le persone fisiche, la scelta di questo particolare strumento si spiega in base al fatto che esso, pur applicandosi esclusivamente alle primissime fasi del trattamento, è in grado di estendere la sua efficacia anche al momento di applicazione del profilo di gruppo. Il *DPIA*, infatti, si connota per una particolare *attenzione* agli effetti del trattamento piuttosto che alle modalità tecniche del suo svolgersi, così trasfigurando l'impostazione prettamente procedurale[97] delle tutele garantite dal

[93] Dello stesso parere Council of Europe, *Discrimination, artificial intelligence, and algorithmic decision-making*: study by F.Z. Borgesius, 2018, 20.

[94] Cfr. *supra*, sez. 2.

[95] Art. 4(1), Reg. EU 679/2016, cit.

[96] Art. 35, Reg. EU 679/2016, cit.

[97] A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment,* in *Computer Law and Security Review*, 34, 2018, 754-772, 761.

GDPR in un sistema decisamente più orientato al risultato finale[98], capace di estendere la sua portata regolatoria a *fatti* non muniti del *requisito della personalità del dato*.
Avendo spiegato in che modo l'effettuazione di un *DPIA* possa astrattamente fungere al nostro scopo, è ora il momento di analizzare, in prima istanza, le condizioni della sua applicabilità e, in secondo luogo, come questo strumento possa, nei fatti, apportare benefici alla condizione dei soggetti sottoposti alla profilazione di gruppo. Per quel che riguarda la prima questione, sappiamo che il titolare *è tenuto ad effettuare* un *DPIA* in particolari casi: quando il trattamento «prevede […] l'uso di nuove tecnologie[99]» e quando questo «può presentare un rischio elevato per i diritti e le libertà delle *persone fisiche* [cors. agg.][100]». Quest'ultimo requisito, in particolare, dovrebbe essere valutato prendendo in considerazione «la natura, l'oggetto, il *contesto* e le *finalità* del trattamento [cors. agg.][101]». Di conseguenza, la valutazione dell'impatto del trattamento dovrebbe basarsi non solo sui rischi che il trattamento presenta *hic et nunc* al momento della valutazione – il che si tradurrebbe, nel caso di specie, nell'affermare la totale assenza di rischi concreti per le persone fisiche, essendo questi successivi al momento in cui il titolare è tenuto ad effettuare il *DPIA* – ma anche sulla considerazione dei rischi che il trattamento potrebbe ragionevolmente porre in futuro sulla base del «contesto[102]» e delle «finalità[103]» del suo svolgersi. Una tale interpretazione è ulteriormente rafforzata dal fatto che la valutazione si riferisce ai rischi per le *persone fisiche*[104] e non agli *interessati al trattamento*, così evitando di ricadere nella cd. *trappola della non personalità* che invece opera nei tre casi precedentemente delineati[105]. A ciò si aggiunga che nell'elencare alcuni casi in cui «la valutazione d'impatto sulla protezione dei dati […] è richiesta in particolare[106]», cita esplicitamente l'eventualità in cui il trattamento si traduca in «una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la *profilazione*, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette *persone fisiche*[107]». Ciò considerato, non può esservi ragion di dubbio sull'applicabilità dell'art. 35 al caso di specie: l'esplicito riferimento alle *persone fisiche* – piuttosto che agli *interessati al trattamento* – consente di estendere l'ambito di considerazione dei rischi oltre gli stretti confini della *personalità* del dato.

[98] *Ibid.*
[99] Art. 35, par. 1, Reg. EU 679/2016, cit.
[100] *Ibid.*
[101] *Ibid.*
[102] *Ibid.*
[103] *Ibid.*
[104] *Ibid.*
[105] Cfr. *supra*, sez. 2.1 e 2.2.
[106] Art. 35, par. 3, Reg. EU 679/2016, cit.
[107] *Ibid.*

Chiarita la questione dell'*applicabilità* dell'art. 35 al caso di specie, tocca ora addentrarci nelle questioni attinenti alla sua *applicazione*. In sostanza, accertata la possibilità di applicare le regole in materia di *DPIA*, la domanda a cui ora tocca rispondere è se queste siano effettivamente in grado, anche in assenza del requisito della *personalità del dato,* di smussare gli effetti dannosi della profilazione di gruppo. La risposta è complessa. Anzitutto, va considerato che i vantaggi dell'effettuazione di un *DPIA* non risiedono nella creazione di un diritto immediatamente attivabile in capo agli individui coinvolti dal trattamento ma, piuttosto, nella creazione, in capo al titolare del trattamento (*melius,* dopo la generazione del profilo e l'anonimizzazione dei dati: l'applicatore del profilo), di una serie di doveri. Anzitutto, è obbligato a descrivere in modo sistematico i trattamenti previsti[108] ed esporre le «misure previste per affrontare i rischi[109]» tenendo conto non solo «dei diritti e degli interessi legittimi degli interessati[110]» ma anche di quelli «*delle altre persone in questione*[111]». Ovviamente, sarà poi suo dovere proseguire il trattamento dei dati in conformità alle misure così delineate.

I vantaggi di questo sistema sono evidenti: il titolare del trattamento (poi, applicatore del profilo) è tenuto a considerare, *prima che il trattamento abbia luogo*, i suoi potenziali effetti negativi sui diritti delle *persone fisiche*, e, conseguentemente, ha anche l'obbligo legale di adoperarsi per evitare tali conseguenze dannose. In pratica, il titolare, *appena* entra in contatto con i dati – *ancora* – personali dalla cui aggregazione e *de-personalizzazione* verrà generato il profilo di gruppo, è obbligato a prendere tutte le "misure tecniche e organizzative" necessarie affinché i possibili effetti negativi del trattamento siano evitati e, nel caso in cui comunque persista il rischio di tali conseguenze dannose, ad astenersi dal trattamento dannoso, *id est* bloccare il trattamento di tali dati prima della generazione e dell'applicazione dei profili). Quale sia la natura delle misure "tecniche e organizzative" adeguate e quali siano le voci da considerare all'interno del DPIA[112] è, ovviamente, materia di grande discussione[113], ma, perlomeno, un sentiero percorribile verso l'obiettivo di regolare anche le conseguenze *stricto iure* non-personali del trattamento è stato aperto: pur circoscrivendo l'applicazione dell'articolo ad un momento del trattamento che precede l'effettivo realizzarsi delle conseguenze dannose, siamo comunque in grado di ricompren-

[108] Art. 35, par. 7, Reg. EU 679/2016, cit.

[109] *Ibid.*

[110] *Ibid.*

[111] *Ibid.*

[112] Si veda, ad esempio, European Union Agency for Fundamental Rights (FRA), *Preventing Unlawful profiling today and in the future: a guide*, 2018, 80.

[113] Si veda, ad esempio, T. Calders – S. Verwer, *Three naive Bayes approaches for discrimination-free classification,* in *Data Mining and Knowledge Discovery*, 2010, 21, 277-292; S. Hajian *et al.*, *Rule protection for indirect discrimination prevention in data mining,* in *Modeling Decision for Artificial Intelligence*, 2011, 211-222; F. Kamiran – T.Calders, *Data Pre-processing Techniques for Classification without Discrimination*, in *Knowledge and Information Systems*, 33, 1, 1-33.

dere, nella propagazione dei suoi effetti, anche le fasi successive – ossia quelle potenzialmente lesive delle persone coinvolte – del trattamento.
Una tale estensione degli *effetti* dell'applicazione dell'art. 35 – ma, *caveat*, non della sua applicazione *per se* – alle conseguenze discriminatorie e alle false applicazioni del profilo di gruppo trova ulteriore supporto nel considerando 71[114]. Questo, infatti, nella sua componente esplicativa del principio di correttezza[115] (*principle of fairness*), afferma che un trattamento di dati può dirsi conforme al principio di correttezza quando tutte le «misure tecniche e organizzative adeguate» affinché sia «minimizzato il rischio di errori[116]» e per garantire che il trattamento venga condotto «secondo una modalità che […] impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche[117]» o «misure aventi tali effetti[118]». È estremamente interessante notare che il cons. 71 riferisce la tutela antidiscriminatoria alle "persone fisiche" in generale: nonostante il riferimento trattamento di dati *personali,* il soggetto dell'indicazione offerta dal considerando non è l'interessato al trattamento. Non v'è dubbio che l'aver reso oggetto specifico di protezione la *persona fisica* sia una lodevole deviazione dall'equazione – presente, in filigrana, in ogni previsione del Regolamento – tra *personalità* del dato e presenza di un rischio per le persone fisiche. Inoltre, la formulazione di questo considerando, facendo esplicita menzione del rischio di applicazioni false o discriminatorie del profilo di gruppo – tema ripreso, anche se meno esplicitamente, anche da altre previsioni[119] del Regolamento – dimostra che tali conseguenze potenziali godono, nell'occhio del legislatore, di una considerazione privilegiata e, dunque, che è bene che siano prese in specifica considerazione nel valutare l'impatto del trattamento dei dati. Sfortunatamente, non v'è una risposta altrettanto specifica al problema dell'inapplicabilità delle salvaguardie dell'art. 22 alle decisioni automatizzate prese a livello di gruppo sulla base di *shared-identity proxies* che non consentono di *distinguere singolarmente* i soggetti che vi sono sottoposti. In ogni caso, la via qui proposta è in grado di apportare benefici tangenziali anche in tali casi: pur nella non attuabilità delle tutele conferite dall'art. 22, vi sarà almeno modo di proteggerli, se del caso, dalle ripercussioni più dannose di tali decisioni, ovverosia il rischio di discriminazione e le applicazioni errate del profilo di gruppo.
Un ultimo punto è da considerare. Si potrebbe, infatti, credere che la soluzione proposta in questa sede sia *de facto* comparabile alla cd. "valutazione d'impatto sui diritti umani[120]" (*HRIA*). Tuttavia, i due strumenti, pur se simili nelle finalità, presentano fondamentali differenze. Anzitutto, il grandissimo vantaggio dell'applicazione dell'art. 35 è il fatto della sua

[114] Cons. 71, Reg. EU 679/2016, cit.
[115] *Ivi,* art. 5, par. 1.
[116] *Ivi,* Cons. 71.
[117] *Ibid.*
[118] *Ibid.*
[119] si veda, ad esempio, il cons. 75, Reg. EU 679/2016, cit.
[120] United Nations, *Guiding Principles on Business and Human Rights*, art. 18-19.

coercibilità: l'effettuazione della valutazione dei rischi del trattamento non è rimessa alla "buona volontà" dei soggetti che implementano tali pratiche, ma è espressamente richiesta dalla legge al verificarsi di alcune condizioni, le quali, come emerso, saranno tendenzialmente sempre presenti nel caso della profilazione di gruppo. La coercibilità della valutazione è ulteriormente rafforzata dalla presenza di una Autorità di controllo *ad hoc* (*DPA*), la quale deve essere opportunamente informata dei risultati della valutazione d'impatto[121] e che, se opportuno, può utilizzare i poteri coercitivi di cui è provvista ai sensi dell'art. 58[122].
Inoltre, nelle autorevoli parole di numerose Istituzioni europee[123], ritroviamo spunti che evidenziano una tendenza a voler superare i limiti della disciplina in materia di protezione dei dati personali orientando il sistema di protezione verso una maggiore considerazione degli effetti pratici e del loro impatto materiale sulle persone fisiche e sulla società in generale[124].
La "volontà di andare oltre i limiti della *data protection law*[125]" significherebbe, dunque, abbandonare le attuali forme di tutela esclusivamente *procedurali* – cioè attivabili sulla base delle modalità con cui è svolto il trattamento e non delle conseguenze che questo comporta – per sperimentare un approccio più orientato alle circostanze di fatto e al raggiungimento degli obiettivi[126] che il GDPR, nel concreto, si è imposto. L'utilizzo dell'art. 35 si inserisce pienamente in questa tendenza: regola *direttamente* gli effetti del trattamento e agisce sulle sue conseguenze, a prescindere dalle procedure e dai mezzi – *personali* o *non personali* – che ne sono stati causa.

Considerazioni conclusive

Ripercorrendo l'*iter* di analisi che questo contributo ha tracciato, vi sono alcune puntualizzazioni che non possiamo esimerci dal compiere. Anzitutto, abbiamo evidenziato l'inadeguatezza della definizione della nozione di dato personale alla finalità di tutela per cui questa è stata disegnata. Come già detto, la radice della discrepanza tra *finalità ideale* della nozione ed il suo *effetto concreto* è da ricercarsi nella mancata aderenza alla realtà dell'equazione fondamentale che regge l'architettura del GDPR: il concetto di personalità del dato non sembra essere unità di misura idonea a individuare concretamente tutte le situazioni di rischio

[121] Art. 36, par. 1, Reg. EU 679/2016, cit.

[122] Art. 58, Reg. EU 679/2016, cit.

[123] EAG (EDPS), Report 'Towards a digital ethics', 2018; Art. 29 Working Party, WP 248 rev. 01, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679,* 4 ottobre 2017.

[124] A. Mantelero, *Towards a Big Data regulation based on social and ethical values. The guidelines of the Council of Europe,* in *Revista de Bioética y Derecho,* 2017.

[125] EAG (EDPS), cit.; WP 248 rev.01, cit.; A. Mantelero, *AI and Big Data*, cit.

[126] A. Mantelero, *AI and Big Data*, cit.

create dal trattamento dei dati. A fronte della flessibilità con cui è delineato il contenuto del dato («qualsiasi informazione[127]») e della elasticità con cui va a definirsi il rapporto tra dato e soggetto (semplicemente «riguardante[128]» per «contenuto, […] risultato o […] finalità[129]»), si staglia la rigidità dei requisiti "nascosti" della nozione di dato personale intravisti fra i "non detti" del Regolamento e degli interventi della WP29 recepiti dallo EDPS: la *singolarità* e la *distinguibilità* della persona fisica, direttamente discendenti dal requisito dell'*identificabilità*. Sulla base dell'assunto individualistico[130] che solo in presenza di questi requisiti si possa creare una situazione di pericolo, l'interessato al trattamento figura come il "grande assente" della profilazione di gruppo: il soggetto che *non c'è*, il soggetto che *non è* – sarebbe azzardato parlare di soggetto in senso giuridico in mancanza di *singolarità* e *distinguibilità* – eppure vede i suoi diritti e le sue libertà[131], nonché la sua identità, in pericolo. Con nuova consapevolezza torniamo, dunque, a parlare della discrasia tra la nozione di *personalità* e il concetto di *identità* e della conseguente *trappola della non personalità*, sul presupposto – non verificabile e sicuramente non verificato – che *identificazione* e *identità* siano nozioni interscambiabili figlie della stessa matrice e, conseguentemente, che il concetto di *personalità di un dato* – ossia, tra le altre cose, *singolarità* e *distinguibilità* del soggetto cui è riferito e quel che usiamo intendere quando parliamo di *identità*[132] siano, uno per l'altro, unità di misura e cifra esplicativa. Potremmo quasi credere di essere riusciti a sfuggire a questo cortocircuito – se non per quel che riguarda la mancata coercibilità degli obblighi informativi necessari a garantire la corretta applicazione del principio di trasparenza, almeno a proposito delle conseguenze dannose del trattamento stesso; ovviamente, senza dimenticare che l'aver rimesso l'efficacia del Regolamento in un settore tanto importante alla sensibilità dell'interprete e i *girotondi interpretativi* in grado di garantirla alla sua buona volontà, è un *vulnus*, pur se non fatale, sicuramente invalidante per la tenuta del Regolamento.

[127] Art. 4(1), Reg. EU 679/2016, cit.

[128] *Ibid.*

[129] WP 136, *cit.*, 6 and ss.

[130] L. Floridi, *The informational nature of personal identity*, in *Minds and Machines*, 2011. Non è questa la sede idonea a raccontare le ultime tappe della filosofia e degli studi sull'identità, che, concedendo molto alle teorie *organicistiche*, preferiscono parlare dell'identità dell'individuo come risultante della *struttura* in cui questo è immerso e si muove. Si veda anche F.J.Z. Borgesius, *Singling out people without knowing their names: Behavioural targeting, pseudonymous data, and the new Data Protection Regulation*, in *Computer Law & Security Rev.*, 2016.

[131] Come è stato efficacemente detto (L. Taylor – L. Floridi – B.van der Sloot, *op. cit.*, 5): «The fact that the individual is often no longer central, but incidental to these types of processes, challenges the very foundations of most currently existing legal, ethical and social practices and theories».

[132] G. Finocchiaro – A.Ricci, *Quality of Information, the Right to Oblivion and Digital Reputation,* in B.Custers – T.Calders *et al.*, *op. cit.*, 289: «the word "identity" means "all personal attributes as a whole". […] The notion of "personal identity" has been for a long time reduced to that of identification, however starting from the '70s several court decisions began to adopt a totally new concept of identity as a complex of spiritual and moral features which are distinctive of individuals, which express their character and autonomy. Such notion of identity is known as the "identity as a projection" of one's moral and intellectual choices. A most recent evolution of such a concept seems to be that of the identity as the right to build oneself, to choose one's moral and spiritual personality rather than merely projecting it on the outside. In such a sense, identity can be defined as an expression of "moral liberty"».