

# smp

**SOCIETÀ MUTAMENTO POLITICA**  
RIVISTA ITALIANA DI SOCIOLOGIA

Oltre le sociologie.  
Dialoghi interdisciplinari su  
incertezza, rischio  
e vulnerabilità

VOL. 13, N° 25 • 2022  
ISSN 2038-3150

**fi**  
FIRENZE  
UNIVERSITY  
PRESS

**SOCIETÀ MUTAMENTO POLITICA**  
RIVISTA ITALIANA DI SOCIOLOGIA

Oltre le sociologie.  
Dialoghi interdisciplinari su incertezza,  
rischio e vulnerabilità



**REDAZIONE**

|                             |                    |
|-----------------------------|--------------------|
| Lorenzo Viviani (direttore) | Stella Milani      |
| Lorenzo Grifone Baglioni    | Barbara Pentimalli |
| Pierluca Birindelli         | Andrea Pirni       |
| Silvia Cervia               | Ilaria Pitti       |
| Carlo Colloca               | Stefano Poli       |
| Marco Damiani               | Luca Raffini       |
| Simona Gozzo                | Andrea Valzania    |

**COMITATO SCIENTIFICO**

Antonio Alaminos, Universidad de Alicante  
Luigi Bonanate, Università di Torino  
Marco Bontempi, Università di Firenze  
Fermín Bouza †, Universidad Complutense de Madrid  
Enzo Campelli, Università di Roma "La Sapienza"  
Enrico Caniglia, Università di Perugia  
Luciano Cavalli, Università di Firenze  
Vincenzo Cicchelli, Université de la Sorbonne - Paris Descartes  
Vittorio Cotesta, Università di Roma III  
Gerard Delanty, University of Sussex  
Antonio de Lillo †, Università di Milano-Bicocca  
Klaus Eder, Humboldt Universität, Berlin  
Livia Garcia Faroldi, Universidad de Malaga  
Roland Inglehart, University of Michigan  
Laura Leonardi, Università di Firenze  
Mauro Magatti, Università Cattolica di Milano  
Stefano Monti Bragadin, Università di Genova  
Luigi Muzzetto, Università di Pisa  
Massimo Pendenza, Università di Salerno  
Ettore Recchi, Sciences Po, Paris  
M'hammed Sabour, University of Eastern Finland, Finlandia  
Jorge Arzate Salgado, Universidad Autónoma del Estado de México, Mexico  
Ambrogio Santambrogio, Università di Perugia  
Riccardo Scartezzini, Università di Trento  
Roberto Segatori, Università di Perugia  
Sandro Segre, Università di Genova  
Sylvie Strudel, Université Panthéon-Assas Paris-II  
José Félix Tezanos, Universidad Uned Madrid  
Anna Triandafyllidou, European University Institute, Robert Schuman Centre for Advanced Studies  
Paolo Turi, Università di Firenze  
Claudius Wagemann, Goethe University, Frankfurt

Immagine nella pagina precedente: Banksy street art, Nicholas Everitt Park, Lowestoft (UK), 2021

**Copyright © 2022 Authors.** The authors retain all rights to the original work without any restrictions.

**Open Access.** This issue is distributed under the terms of the [Creative Commons Attribution 4.0 International License \(CC-BY-4.0\)](https://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The Creative Commons Public Domain Dedication (CC0 1.0) waiver applies to the data made available in this issue, unless otherwise stated.

*Published by*

**Firenze University Press** – University of Florence, Italy  
Via Cittadella, 7 - 50144 Florence - Italy  
<http://www.fupress.com/smp>

## Oltre le sociologie. Dialoghi interdisciplinari su incertezza, rischio e vulnerabilità

A cura di Andrea Pirni

### Indice

---

- |   |  |
|---|--|
| <p>5 Incertezza, rischio e vulnerabilità. Per un dialogo interdisciplinare<br/><i>Andrea Pirni</i></p> <p>9 L'incertezza europea in tempi di pandemia. Tra la salute e l'economia<br/><i>Antonio Alaminos, Paloma Alaminos-Fernández</i></p> <p>23 Globalizzazione, disuguaglianze e nuovi approcci verso un modello di capitalismo sostenibile<br/><i>Maria Mirabelli, Vincenzo Fortunato, Antonio Martin Artilles</i></p> <p>37 L'ago della discordia. Scienza, politica e contestazione nel dibattito pubblico<br/><i>Luca Raffini, Federico Zuolo</i></p> <p>51 Social media e pandemia. Il Movimento inconsapevole<br/><i>Simona Gozzo, Rosario D'Agata, Giovanni Giuffrida</i></p> <p>63 La pandemia e il paradigma immunitario: le sfide della politica tra sicurezza e solidarietà<br/><i>Antonella Coco</i></p> <p>73 Rischio e vulnerabilità nel modello europeo di intelligenza artificiale<br/><i>Mariavittoria Catanzariti</i></p> <p>83 Il cambiamento climatico e l'impatto sulla salute: le <i>pathoclima</i><br/><i>Roberto Buizza, Francesco Misiti, Alessandra Sannella</i></p> <p>97 La riprogettazione post sisma: verso nuove reti di engagement <i>all-of-society</i><br/><i>Lucia D'Ambrosi, Valentina Polci, Massimo Sargolini</i></p> <p>109 La sostenibilità come paradigma: il caso dell'infrastruttura Metrofood-RI nel settore agroalimentare<br/><i>Mariella Nocenzi, Ombretta Presenti, Claudia Zoani</i></p> <p>121 Il ruolo delle università nella promozione della mobilità sostenibile e inclusiva<br/><i>Ilaria Delponte, Simone Caiello, Luca Daconto</i></p> | <p>133 Pandemia, ibridazione e il ruolo del Terzo settore. Un'analisi sul caso del Banco Alimentare<br/><i>Marco Libbi, Anna Reggiardo</i></p> <p><b>L'intervista</b></p> <p>145 Muoversi fra le discipline per un arricchimento reciproco. Intervista a Marco Aime<br/><i>a cura di Andrea Pirni</i></p> <p>149 Attraversare i confini come vocazione: uno sguardo autobiografico. Intervista a Marco Marzano<br/><i>Andrea Pirni</i></p> <p><b>Passim</b></p> <p>153 Eteronomia versus autonomia. Emergenza e individualizzazione nel primo anno di pandemia in Italia<br/><i>Lorenzo Grifone Baglioni</i></p> <p>161 Oltre la sociologia pubblica e di servizio. Per una sociologia trasformativa e di posizione<br/><i>Fabio de Nardis, Anna Simone</i></p> <p>175 Uno strano oggetto per la sociologia: l'attenzione come processo sociale<br/><i>Enrico Campo</i></p> <p>185 La costruzione del sociale nell'epoca della postrealtà<br/><i>Edmondo Grassi</i></p> <p>195 I politici e l'immigrazione su Facebook: come si (de)legittima il discorso migratorio durante l'emergenza sanitaria<br/><i>Dario Lucchesi, Vincenzo Romania</i></p> <p>213 Trasformazioni sociopolitiche a destra. L'evoluzione da Alleanza Nazionale a Fratelli d'Italia: primi risultati di una ricerca empirica<br/><i>Antonello Canzano Giansante</i></p> |
|---|--|

- 223 **Sociologia politica. Quale ruolo pubblico?**  
*Giulio Moini*
- 235 **European Sentiment in time of crises. The  
point of view of young university students**  
*Mariaeugenia Parito, Ricardo Pérez-Calle, Lucia  
D'ambrosi*
- 247 **Appendice bio-bibliografica su autori e autrici**



**Citation:** Mariavittoria Catanzariti (2022). Rischio e vulnerabilità nel modello europeo di intelligenza artificiale. *Società Mutamento Politica* 13(25):73-82. doi: 10.36253/smp-13804

**Copyright:** © 2022 Mariavittoria Catanzariti. This is an open access, peer-reviewed article published by Firenze University Press (<http://www.fupress.com/smp>) and distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

**Data Availability Statement:** All relevant data are within the paper and its Supporting Information files.

**Competing Interests:** The Author(s) declare(s) no conflict of interest.

## Rischio e vulnerabilità nel modello europeo di intelligenza artificiale

MARIAVITTORIA CATANZARITI

**Abstract.** The contribution explores how the European model on artificial intelligence addresses the relationship between risk analysis and management of automated systems and its impact on the vulnerability factors that the use of certain deceptive techniques determines or increases. The article draws some reflections on the European model that illustrates how risk assessment and management are logically related to data governance choices. Some data governance choices can lead to mitigation of the risk by combining market needs with an anthropocentric approach. As a result of general considerations on the European approach to artificial intelligence systems, the contribution offers the analysis of a case related to the interoperability of European information systems for purposes of security, migration and European border control, focusing on the impact that these systems have on the real life of third country nationals.

**Keywords.** Risk assessment and management, data governance, artificial intelligence, human oversight, interoperability.

### INTRODUZIONE

La proposta di regolamento UE sulla intelligenza artificiale (AI Act) è stata da molti accolta come il risultato dell'approccio tipicamente europeo alla regolazione degli algoritmi. Cosa vi sia di tipicamente europeo in tale approccio si evince dalle formulazioni dei testi ufficiali e meno dalle pratiche, essendo esso in gran parte legato a ciò che viene definito il cuore dell'identità e dei valori antropocentrici europei.

Tradotto in termini operativi, si tratterebbe di una gestione del rischio a geometria variabile combinata con scelte e obblighi di governance dei dati volti primariamente a evitare o limitare effetti decettivi dei sistemi di intelligenza artificiale sugli individui, garantendo al contempo l'affidabilità dei sistemi. Viene immediatamente da chiedersi in che termini possa parlarsi di effetti decettivi e in relazione a cosa un sistema possa ritenersi affidabile. Nel primo caso, occorre ricordare che il modello culturale europeo si è radicato sullo sviluppo della personalità come progetto di edificazione della coscienza in fieri, mentre nel secondo si fa riferimento alla gestione graduale del rischio in relazione a diverse situazioni di vulnerabilità, in altre parole mitigazione del rischio in relazione alla rilevanza del pericolo di effetti negativi sul target. Il compromesso europeo avallerebbe, dunque, l'idea di un'umanità in gene-



rale disposta ad accettare il rischio di manipolazione ad opera delle macchine intelligenti purché tale rischio sia minimizzato?

#### RISCHI DIFFERENZIATI PER MERCATI DIFFERENZIATI O PER DIVERSE UMANITÀ?

A ben guardare, il processo regolatorio dell'intelligenza artificiale in Europa ha una storia singolare, dapprima filtrato attraverso linee guida etiche<sup>1</sup>, macchinosamente conformate ai diritti fondamentali<sup>2</sup>, poi confluito in una proposta di regolamento che sarà direttamente applicabile negli Stati Membri una volta adottato<sup>3</sup>.

Il primo dato che emerge è dunque di sistema: il consenso etico sui valori è frutto di una policy preparatoria rispetto alla regolazione. Entrambi i sistemi di regole, quello etico e quello giuridico, sono stati parametrati sulla base di soglie di accettabilità del rischio dei sistemi di intelligenza artificiale, il che rappresenta di per sé un inedito del modello europeo, tipicamente costruito come modello giuridico *tout-court* nel quale i valori dell'Unione rappresentano il limite di tenuta del sistema al quale istituzioni e individui riferiscono la propria identità "europea".

Si tratta in fin dei conti della nota questione del come coniugare valori, diritti e mercato globale, o di qualcosa di diverso? L'idea più probabile è che ci si sia affidati a due ordini di regole, quelle etiche e quelle giuridiche, per differenziare situazioni in relazione al rischio e all'incidenza di esso su fattori di vulnerabilità sociale, non deprimendo irragionevolmente il mercato con un approccio orizzontale regolatorio non diversificato sulla base di differenti situazioni di rischio<sup>4</sup>.

La struttura del regolamento in oggetto, letta nel suo insieme, fornisce indicazioni sulle finalità di un progetto indubbiamente ambizioso.

Il Titolo I ci offre una definizione di intelligenza artificiale tecnologicamente neutrale e sostenibile nel lungo periodo con la previsione dei codici di condotta per sistemi non ad alto rischio; il Titolo II prevede una lista di sistemi di IA proibiti classificandoli in base al rischio: rischio inaccettabile, rischio alto e rischio mini-

mo; il Titolo III prevede specifiche regole per sistemi ad alto rischio che possono comportare rischi alla salute e alla sicurezza nonché ai diritti fondamentali delle persone<sup>5</sup>. I sistemi di IA sono tendenzialmente classificati in due categorie: sistemi volti a essere utilizzati come componenti della sicurezza dei prodotti immessi sul mercato e soggetti a una valutazione di conformità ex ante da parte di terzi; sistemi autonomi che possono avere implicazioni per i diritti fondamentali ed elencati tassativamente. Il Titolo IV prevede obblighi di trasparenza per alcuni sistemi che presentano rischi di manipolazione. Sono previsti per quei sistemi che interagiscono con gli umani, che identificano emozioni e determinano associazioni con categorie sociali essendo basati su dati biometrici, generano o manipolano i contenuti (*deep fakes*). Il Titolo V contribuisce a creare un framework giuridico incoraggiando le autorità nazionali a dotarsi di un *sandbox* regolatorio in termini di supervisione, governance e responsabilità. Il Titolo VI diversifica i sistemi di governance a livello europeo e nazionale. A livello interno gli Stati Membri devono designare una o più autorità competenti, mentre lo European Data Protection Supervisor sarà autorità competente per la supervisione delle istituzioni EU. Il Titolo VII prevede programmaticamente la creazione di un grande database che include i sistemi di IA autonomi che hanno impatto sui diritti fondamentali. Il Titolo VIII include obblighi di monitoraggio e reporting per i providers con riguardo al post-market monitoring; il Titolo IX crea un framework di obblighi di condotta per i sistemi non ad alto rischio volto al supporto volontario di meccanismi di sostenibilità, accesso di disabili e diversità. Infine, i Titoli X, XI e XII contengono le norme finali volte a far rispettare la confidenzialità delle informazioni e dei dati; l'esercizio della delega e dei poteri di implementazione; infine, l'obbligo per la Commissione di aggiornamento della lista dei sistemi IA ad alto rischio previsti nell'allegato III del Regolamento.

Tuttavia, il regolamento non contiene alcuna indicazione dei rimedi giuridici contro gli effetti avversi dei sistemi di intelligenza artificiale. Come bisogna interpretare questa assenza? Nel senso che il legislatore europeo, anch'esso intelligente, abbia calcolato l'assenza di danni e per questo non abbia inserito alcuna disposizione sui diritti individuali e le azioni esperibili davanti a un giudice, oppure nel senso che la previsione dei rimedi in realtà non è scelta razionale rispetto allo sviluppo del mercato?

Partendo dalla definizione di intelligenza artificiale contenuta nella proposta di Regolamento AI (Art.

<sup>1</sup> AI HLEG, Orientamenti etici per una IA affidabile, <https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html>.

<sup>2</sup> Catanzariti M. (2021), *Etica "artificiale": un nuovo modello regolatorio?*, in «Ars Interpretandi», 1: 165-179.

<sup>3</sup> Proposta di regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final, (di seguito, AI Act).

<sup>4</sup> Per una trattazione approfondita si veda Mantelero A. (2022), *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, Springer, The Hague.

<sup>5</sup> I sistemi ad alto rischio sono elencati tassativamente nell'allegato III dell'AI Act. Nello specifico, si rimanda alle pp. 77 e 78 e alla nota n. 23.

3, n. 1), che definisce “sistema di intelligenza artificiale” (sistema di IA) «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono», emergono due tratti essenziali. Da un lato la previsione degli obiettivi del sistema da parte dell'uomo, dall'altro la produzione di effetti su contesti circostanti.

Una delle caratteristiche peculiari del modello europeo risiede nel fatto che le previsioni umane possono influenzare i contesti con i quali i sistemi interagiscono nella misura in cui la gestione del rischio sia costante e messa in atto mediante un “processo iterativo continuo eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio”<sup>6</sup>. Tale gestione comprende diverse fasi, fra le quali la valutazione e l'analisi dei rischi noti e prevedibili, l'analisi dei rischi specifici sia in caso di funzionamento conforme alle finalità previste sia in caso di uso improprio, l'adozione di adeguate misure<sup>7</sup>. Tuttavia, calcolo del rischio significa determinazione di una soglia di accettabilità di un sistema informazionale che si innesta all'interno di un sistema capitalistico rappresentato dal cosiddetto *Digital Single Market*. Tale modello mira a creare un ambiente favorevole per l'accesso di imprese e consumatori a network, beni e servizi digitali.

L'accettabilità o meno del rischio è parametrata a un funzionamento del sistema ad alto rischio sempre in conformità alle finalità previste o in condizioni di uso improprio ragionevolmente prevedibile<sup>8</sup>. Assieme ai rischi peculiari dei singoli sistemi, vi sono anche rischi residui la cui possibilità di riduzione e/o limitazione è parametrata alla capacità informativa dell'utente, alle sue conoscenze tecniche, alla sua esperienza, istruzione e formazione. Tuttavia, la gestione del rischio è strettamente connessa al sistema di gestione dei dati di addestramento, convalida e prova dei sistemi ad alto rischio<sup>9</sup>,

specie quando un sistema ad alto rischio – quali ad esempio quelli destinati a essere utilizzati per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica ovvero l'affidabilità creditizia e il merito di credito – è sviluppato sulla base di data set di questo tipo<sup>10</sup>.

Tra le caratteristiche necessarie di questi set di dati, vi sono la pertinenza, la rappresentatività, la mancanza di errori e la completezza. La pertinenza riguarda le scelte progettuali, la raccolta, le operazioni di trattamento, la formulazione delle ipotesi, la valutazione della disponibilità, della quantità e dell'adeguatezza di dati. La rappresentatività invece indica l'insieme delle proprietà statistiche adeguate a rappresentare dati relativi a gruppi di persone. Inoltre, i sistemi ad alto rischio devono avere una rilevanza di contesto, geografico, comportamentale o funzionale.

Ciò che emerge dall'approccio combinato tra analisi e gestione del rischio e scelte di data governance è il carattere relazionale dell'utilizzo dei dati in rapporto a tendenze generalizzate, la cui massimizzazione in termini economici può comportare un pregiudizio sociale. Il danno può essere rappresentato non soltanto dalle interferenze nelle modalità di autoformazione del soggetto, ma dal contesto delle relazioni che determinano o amplificano fattori di disuguaglianza sociale<sup>11</sup>. L'opportunità offerta da un'analisi del rischio modellata su scelte di data governance solide si concretizza in un'ambizione di un nuovo ordine sociale che accoglie la sfida della strategia digitale nella misura in cui essa non valichi limiti inaccettabili.

In relazione alla vulnerabilità, invece, v'è da osservare come la gestione del rischio sia volta a fronteggiare una serie di fenomeni che possono determinare situazioni diverse. Difatti, la proposta di regolamento bandisce, ad esempio, le pratiche di intelligenza artificiale che utilizzano tecniche subliminali o sfruttano la vulnerabilità di un determinato gruppo in relazione all'età o alla disabilità al fine di distorcere il comportamento umano in modo tale che esso possa provocare un danno fisico

<sup>6</sup> Art. 9, par. 2 AI Act.

<sup>7</sup> Art. 9, par. 2 (lett. a, b, c, d) AI Act.

<sup>8</sup> Art. 9, par. 4.

<sup>9</sup> Secondo le definizioni di cui all'art. 3 AI Act, per dati di addestramento si intendono i dati utilizzati per addestrare un sistema di IA adattandone i parametri che può apprendere, compresi i pesi di una rete neurale; i dati di convalida sono i dati utilizzati per fornire una valutazione del sistema di IA addestrato e per metterne a punto, tra l'altro, i parametri che non può apprendere e il processo di apprendimento, al fine di evitare l'eccessivo adattamento ai dati di addestramento (*overfitting*), considerando che il set di dati di convalida può essere un set di dati distinto o essere costituito da una partizione fissa o variabile del set di dati di addestramento; i dati di prova vengono invece definiti come i dati utilizzati per fornire una valutazione indipendente del sistema di IA addestrato e convalidato al fine di confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio.

<sup>10</sup> Tra le pratiche di gestione e governance dei dati si annoverano ad esempio le scelte progettuali pertinenti; la raccolta dei dati; le operazioni di trattamento pertinenti ai fini della preparazione dei dati, quali annotazione, etichettatura, pulizia, arricchimento e aggregazione; la formulazione di ipotesi pertinenti, in particolare per quanto riguarda le informazioni che si presume che i dati misurino e rappresentino; una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari; un esame atto a valutare le possibili distorsioni; l'individuazione di eventuali lacune o carenze nei dati e il modo in cui tali lacune e carenze possono essere colmate, si veda Art. 10, par. 2 (lett. a, b, c, d, e, f, g).

<sup>11</sup> Viljoen S. (2021-22), *A Relational Theory of Data Governance*, in «The Yale Law Journal», 131: 573-653.



o psicologico<sup>12</sup>; il cosiddetto *social scoring* da parte delle autorità pubbliche (si badi non da parte dei privati!) che determini un trattamento sfavorevole o pregiudizievole in contesti sociali non collegato a quelli nei quali avviene la raccolta o ingiustificato e sproporzionato; l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico per finalità di contrasto al crimine salvo che al ricorrere di specifiche condizioni (ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi; la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato nel contesto di una procedura di mandato di arresto europeo) e comunque previa autorizzazione giudiziaria o amministrativa ed entro specifici limiti temporali, geografici e personali previsti dalla normativa dei singoli Stati Membri<sup>13</sup>.

Il tutto meriterebbe plausibile placet, se non fosse per una piccolissima chiosa relativa all'ambito di applicazione: il regolamento si applica a tutti i sistemi di intelligenza artificiale che "generino output" nel mercato europeo, ma non ai sistemi prodotti nell'UE e immessi in altri mercati! Inoltre, non si applica in alcun caso a sistemi di intelligenza artificiale per scopi militari né alle autorità pubbliche in paesi terzi che operano per finalità di contrasto a reati sulla base di accordi internazionali<sup>14</sup>.

In altri termini, sembrerebbe che gli Europei amino sentirsi Europei in Europa!

## NUMERI O VALORI?

Il modello prescelto nella proposta di regolamento è quello relativo a uno strumento di legislazione che segue un approccio proporzionato basato sul rischio, affiancato da previsione di codici etici per i sistemi non ad alto rischio. I modelli al vaglio della Commissione che sono stati scartati nel testo licenziato sono invece: 1) strumento legislativo che mette a punto uno schema volontario di etichettatura volontario; 2) approccio settoriale ad hoc; 3) strumento di legislazione con proporzionata valutazione del rischio *tout court*; 4) strumento di legislazione orizzontale che stabilisca requisiti obbligatori per tutti i sistemi IA a prescindere dal rischio posto. La scelta è stata fatta sulla base dell'impatto economico e sociale, e in particolare dell'impatto sui diritti fonda-

mentali, con l'obiettivo di mantenere i costi di conformità al minimo<sup>15</sup>.

Come osserva Pietro Rossi, «al di là di una certa soglia gli algoritmi continuano a funzionare, ma il diritto diventa impotente»<sup>16</sup>. In un certo senso, in relazione alle tecnologie *data-driven* il diritto è in fin dei conti un sistema di valori e non di numeri<sup>17</sup>. Tuttavia, sia le infrastrutture digitali sia le reti di comunicazione sia gli istituti giuridici si trovano a metà tra verità e potere e hanno un carattere ambivalente<sup>18</sup>. Possono, cioè sia essere mezzi di emancipazione sia incubatori di pratiche di potere. Questa ambivalenza risiede nella loro capacità di autorizzare, trasmettere e modulare flussi informativi e schemi comportamentali di fatto "mediando" tra verità e potere<sup>19</sup>.

La regolazione affidabile a vari livelli e servente rispetto alla impresa capitalistica rappresenta la matrice del razionalismo occidentale, che ben si adatta chiaramente a qualsiasi oggetto, si tratti o meno di algoritmi. Sempre Pietro Rossi, riprendendo Max Weber, sostiene che il suo valore aggiunto consiste nel coniugare razionalità formale e razionalità materiale<sup>20</sup>, la prima designando «la misura del calcolo tecnicamente possibile e realmente applicabile», la seconda indicando «il grado in cui l'approvvigionamento di determinati gruppi umani [...] con determinati beni [...] viene a configurarsi dal punto di vista di determinati postulati valutativi» vale a dire «esigenze etiche, politiche, utilitarie, edonistiche, di ceto, di eguaglianza o di qualsiasi altra specie».

Un mosaico interessante, dunque, quello della rego-

<sup>15</sup> AI Act, [https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC_1&format=PDF), 10.

<sup>16</sup> Rossi P. (2017), cit., 36.

<sup>17</sup> Cfr Zeno Zencovich V. (2017), *Ten Legal Perspectives on the "Big Data Revolution"*, Editoriale Scientifica, Napoli 2017, p. 53, in netta contrapposizione alla tesi di Natalino Irti, in A. Carleo (a cura di) *Per un dialogo sulla calcolabilità giuridica*, il Mulino, Bologna, pp. 17 ss.

<sup>18</sup> Il dibattito sul tema è sterminato. In questa sede ci si limita a citare soltanto alcuni lavori significativi: Popitz H. (1990), *Fenomenologia del potere. Autorità, violenza, dominio, tecnica*, il Mulino, Bologna; Ceri P. e Borgna P. (1996), *La tecnologia per il XXI° sec. Prospettive di sviluppo e rischi di esclusione*, Einaudi, Torino; Gallino L. (2007), *Tecnologia e democrazia. Conoscenze tecniche e scientifiche come beni pubblici*, Torino, Einaudi; Magatti M., *La libertà immaginaria. Le illusioni del capitalismo techno-nichilista*, Feltrinelli, Milano; Foucault M. (2016), *Il coraggio della verità. Il governo di sé e degli altri II. Corso al Collège de France (1984)*, Feltrinelli, Milano; Zuboff S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma; Golia A. e Teubner G. (2021), *Networked statehood: an institutionalised self-contradiction in the process of globalisation?*, *Transnational Legal Theory*, 1-37.

<sup>19</sup> Cohen J. (2019), *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press, Oxford, p. 5.

<sup>20</sup> Rossi P. (2017), *Razionalismo occidentale e calcolabilità giuridica* in A. Carleo (a cura di), *Calcolabilità giuridica*, il Mulino, Bologna, pp. 29 ss., pp. 30 e 31.

<sup>12</sup> Si veda Malgieri G. e Niklas J. (2020), *Vulnerable Data Subjects*, in «Computer Law & Security Review», 37: 105415.

<sup>13</sup> Art. 5 AI Act.

<sup>14</sup> Art. 2, parr. 1 e 2 AI Act.

lazione del rischio là dove la misura del calcolo, nel limitare fattori di vulnerabilità, riesce in ogni caso a promuovere i valori dell'identità europea offrendo all'Europa una sponda credibile per partecipare alla rosa degli attori tecnologici internazionali.

L'Europa – o il suo mito – tenta dunque di partecipare a quel processo che Julie Cohen ha definito con il nome di capitalismo informazionale nel quale il capitalismo come modalità di produzione e l'informazionalismo come modalità di sviluppo corrono di pari passo, il primo massimizzando i profitti sulla base del controllo privato sui mezzi di produzione e circolazione, il secondo mediante l'accumulazione di conoscenza a livelli di complessità sempre più elevata. Enfatizza l'Autrice: «In a regime of informational capitalism, market actors use knowledge, culture, and networked information technologies as means of extracting and appropriating surplus value, including consumer surplus» (Cohen 2019: 5-6).

La modalità con la quale il capitalismo informazionale opera non differenzia le situazioni e i soggetti perché razionalmente persegue il suo scopo in maniera indipendente dal contesto. Ad esso la sfida europea tenta di porre un macro-limite costituito dal divieto di talune pratiche di intelligenza artificiale, ovvero una razionalità alternativa il cui scopo consiste nell'evitare che l'umanità imploda a causa delle macchine, il cosiddetto approccio antropocentrico<sup>21</sup>. L'approccio antropocentrico, baluardo del modello europeo sia nella sua declinazione etica sia in quella giuridica, si basa essenzialmente sulla possibilità di sorveglianza umana nei sistemi ad alto rischio, sul presupposto che il fornitore dei servizi di intelligenza artificiale predisponga specifiche misure prima dell'immissione del sistema nel mercato. Attraverso queste misure, l'individuo dovrebbe essere in grado in qualsiasi momento di mettere in atto azioni atte a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali, mediante facoltà apparentemente umane, tra le quali la comprensione piena della capacità e dei limiti dei sistemi, la consapevolezza del rischio di un automatico affidamento nel sistema, la corretta interpretazione dei risultati, la libera decisione in ogni stadio di non utilizzare il sistema e la possibilità di arrestarlo interrompendo il suo funzionamento<sup>22</sup>.

<sup>21</sup> Nella teoria dei sistemi, tale approccio rappresenterebbe un'ipotesi di differenziazione funzionale in relazione ai limiti di compatibilità tra diritto e tecnica. Cfr Luhmann N. (1990), *La differenziazione del diritto. Contributi alla sociologia e alla teoria del diritto*, il Mulino, Bologna.

<sup>22</sup> Le misure di sorveglianza umana elencate sono di cinque tipi: «a) comprendere appieno le capacità e i limiti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, in modo che i segnali di anomalie, disfunzioni e prestazioni inattese possano essere individuati e affrontati quanto prima; b) restare consapevole della possibile tendenza a fare automaticamente affidamen-

La possibilità di non aderire al sistema rappresenta dunque la massima alternativa che l'individuo può adottare, modulabile nel rifiuto di quel dato sistema o nella sostituzione con uno migliore. Il senso di una strategia di exit consiste dunque nella scelta possibile di una tecnologia che sia funzionale alle capacità dell'intelletto umano, la cui perfezionabilità fiduciosamente incide sulla speranza di ridurre il più possibile i rischi.

Le pratiche di intelligenza artificiale ad alto rischio sono elencate in un allegato alla proposta, che potrà essere successivamente modificato dalla Commissione. Attualmente esse coinvolgono i settori seguenti: 1) identificazione biometrica e categorizzazione delle persone fisiche; 2) gestione e funzionamento delle infrastrutture critiche (ad esempio i sistemi di IA destinati ad essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento del traffico stradale e nella fornitura di acqua, gas, riscaldamento ed elettricità; 3) istruzione e formazione professionale (tra cui i sistemi aventi lo scopo di determinare l'accesso o assegnare persone fisiche agli istituti di istruzione e formazione professionale o determinare l'accesso di studenti presso istituti di formazione); 4) occupazione, gestione dei lavoratori e accesso al lavoro autonomo (sistemi utilizzati per assunzione e selezione, promozione e risoluzione di rapporti di lavoro); 5) accesso e fruizione dei servizi privati essenziali e dei servizi e benefici pubblici (benefici di prestazione e servizi di assistenza pubblica, valutazione del merito creditizio o della priorità nell'invio di servizi di pronto intervento di emergenza, compresi i vigili del fuoco e l'assistenza medica); 6) forze dell'ordine (valutazioni individuali del rischio di recidiva o per potenziali vittime, rilevamento dello stato emotivo di una persona fisica, valutazione dell'affidabilità delle prove nel corso delle indagini o del perseguimento di reati, tecniche di profilazione delle persone fisiche, l'analisi della criminalità riguardante le persone fisiche e basata su data set di grandi dimensioni, correlati e non correlati, disponibili in diverse fonti di dati o in diversi formati di dati al fine di identificare modelli sconosciuti o scoprire relazioni nascoste nei dati); 7) gestione dell'immigrazione, dell'asilo e del controllo delle frontiere (tra

to o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio ("distorsione dell'automazione"), in particolare per i sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; c) essere in grado di interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto in particolare delle caratteristiche del sistema e degli strumenti e dei metodi di interpretazione disponibili; d) essere in grado di decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio; e) essere in grado di intervenire sul funzionamento del sistema di IA ad alto rischio o di interrompere il sistema mediante un pulsante di "arresto" o una procedura analoga», Art. 14 AI Act (lett. a, b, c, d, e).

questi, sistemi destinati ad essere utilizzati dalle autorità pubbliche competenti come poligrafi e strumenti simili o per rilevare lo stato emotivo di una persona fisica, per valutare un rischio, compreso un rischio per la sicurezza, un rischio di immigrazione irregolare o un rischio per la salute, rappresentato da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro, per verificare l'autenticità dei documenti di viaggio e della documentazione giustificativa delle persone fisiche e per individuare i documenti non autentici verificandone le caratteristiche di sicurezza, per procedere all'esame delle domande di asilo, visti e permessi di soggiorno e relativi reclami per quanto riguarda l'ammissibilità delle persone fisiche che richiedono uno status); 8) amministrazione della giustizia e processi democratici (sistemi di assistenza a un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione del diritto a un insieme concreto di fatti)<sup>23</sup>.

#### UN CASO DI SISTEMA AD ALTO RISCHIO: LA INTEROPERABILITÀ DEI SISTEMI INFORMATIVI EUROPEI

Nella casistica attuale dei sistemi ad alto rischio, particolare attenzione meritano i sistemi utilizzati nella gestione della migrazione, dell'asilo e del controllo delle frontiere poiché essi hanno effetti su persone che si trovano spesso in una posizione particolarmente vulnerabile e il cui futuro dipende dall'esito delle azioni delle autorità pubbliche competenti. L'accuratezza, la natura non discriminatoria e la trasparenza dei sistemi di IA utilizzati in tali contesti sono pertanto particolarmente importanti per garantire il rispetto dei diritti fondamentali delle persone interessate, in particolare i loro diritti alla libera circolazione, alla non discriminazione, alla protezione della vita privata e dei dati personali, alla protezione internazionale e alla buona amministrazione.

Alcuni di essi sono utilizzati per assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto e di permesso di soggiorno e dei relativi reclami in relazione all'obiettivo di determinare l'ammissibilità delle persone fisiche che richiedono tale status e l'identificazione delle persone fisiche.

Le iniziative dell'UE sull'IA per le frontiere utilizzano quattro categorie di applicazioni dell'IA: (1) identificazione biometrica (impronta digitale automatizzata e riconoscimento facciale); (2) rilevamento delle emozioni; (3) valutazione algoritmica del rischio; e (4) strumenti di intelligenza artificiale per il monitoraggio, l'analisi e la previsione della migrazione. Varie sono state le iniziati-

ve sui cosiddetti *smart borders*. Si tratta di confini basati sulla capacità di raccogliere ed elaborare dati e scambiare informazioni. La capacità della tecnologia di spostare le frontiere esterne al di fuori dell'Unione o di creare frontiere digitali è uno dei modi in cui il diritto allinea artificialmente i confini politici e giuridici con le frontiere<sup>24</sup>.

La interoperabilità dei database che tutelano la sicurezza dell'Unione Europea ha come target lo status giuridico "transitorio" dei cittadini di paesi terzi – dunque migranti, richiedenti asilo, sospettati di reati – dipendente dal carattere transitorio e mutevole dei loro dati utilizzati dalle autorità pubbliche sulla base di dati aggregati automaticamente da database interoperabili<sup>25</sup>.

L'iniziativa Europea sulla interoperabilità mira a introdurre una politica di interoperabilità cooperativa per un settore pubblico modernizzato. Grazie a un programma di finanziamento dell'Unione che si è svolto dal 2016 al 2021, essa ha sostenuto lo sviluppo di soluzioni digitali per consentire l'interoperabilità di servizi pubblici transfrontalieri e intersettoriali. Nel maggio 2019 il legislatore dell'UE ha adottato due importanti regolamenti che stabiliscono un quadro uniforme per l'interoperabilità tra i sistemi informativi specifici europei nel campo della cooperazione di polizia e giudiziaria, dell'asilo e della migrazione e nel settore delle frontiere e dei visti.

I regolamenti gemelli (UE) 2019/817 e (UE) 2019/818 hanno stabilito regole di interoperabilità tra i sistemi di informazione europei in materia di frontiere e visti nonché in materia di cooperazione di polizia e giudiziaria, asilo e migrazione. L'obiettivo fondamentale è quello di facilitare la corretta identificazione delle persone, comprese le persone sconosciute e le persone che non sono in grado di identificarsi. L'interoperabilità copre i tre sistemi centralizzati esistenti (Schengen Information System – SIS, Visa Information System – VIS e European Dactiloscopia – Eurodac) e i tre sistemi in fase di sviluppo (Entry Exit System – EES, European Travel Authorization System – ETIAS e Conviction information on third-country nationals and stateless persons – ECRIS-TCN).

La logica sottesa a questa iniziativa consiste nel fatto che le guardie di frontiera, le autorità doganali, gli agenti di polizia e le autorità giudiziarie negli Stati membri necessitano di un accesso più facile ai dati personali per motivi operativi al fine di svolgere i loro compiti<sup>26</sup>. La

<sup>24</sup> Dumbrava C. (2021), *Artificial Intelligence at EU Borders: Overview of Applications and Key Issues*, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRSIDA\(2021\)690706EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRSIDA(2021)690706EN.pdf), (last visited 10 September 2021).

<sup>25</sup> Catanzariti M. (2019), *Individuals or 'bare data'? Unowned Data for Interoperable Borders*, <https://migrationpolicycentre.eu/individuals-or-bare-data/>.

<sup>26</sup> Vavoula N. (2021), *Interoperability of EU Information Systems in a "Panopticon" Union: A Leap Towards Maximised Use of Third-Country*

<sup>23</sup> Allegato III, AI Act.

condivisione delle informazioni è integrata attraverso sei banche dati che sono rese interoperabili tramite quattro componenti: un portale di ricerca europeo, un servizio di corrispondenza biometrica condiviso, un archivio comune di identità e un rilevatore di identità multiple. Le componenti interoperabili riguardano anche i dati della polizia europea Europol, ma soltanto nella misura in cui essi consentano di interrogare i dati Europol contemporaneamente da parte degli altri sei sistemi di informazione dell'UE. Gli obiettivi principali dell'interoperabilità in questo sistema sono salvaguardare la sicurezza a livello degli Stati membri e nell'Area di libertà, sicurezza e giustizia, garantire l'efficacia della gestione delle frontiere e combattere l'immigrazione illegale e i reati gravi. Questi obiettivi saranno realizzati attraverso l'identificazione delle persone, che richiedono il trattamento di un'enorme quantità di dati personali nei sistemi informativi dell'UE che possono basarsi su "identità diverse o incomplete".

Una delle variabili più rilevanti che influenzano le relazioni di potere consiste nell'asimmetria nell'utilizzo dei dati da parte di quegli utenti che originano dati da condividere con altri "utenti" specifici, ovvero le pubbliche autorità competenti. I diritti alla protezione dei dati dei cittadini di paesi terzi sono fortemente limitati in quanto i regolamenti sull'interoperabilità forniscono loro con riguardo al trattamento dei loro dati soltanto diritti di informazione, diritto di accesso, rettifica o cancellazione<sup>27</sup>. Tuttavia, gli interessati dovrebbero sapere se i loro dati sono inclusi all'interno di componenti interoperabili e anche chi ha originato i loro dati personali in quella forma al fine di esercitare pienamente i loro diritti di informazione. Inoltre, non tutti i dati archiviati nelle banche dati sono accessibili agli utenti di sistemi informativi interoperabili, i quali possono accedere soltanto ai dati delle autorità che ne sono in possesso (o abbinati ad altri dati in loro possesso). Se, ad esempio, uno dei database interoperabili origina alcuni dati che vengono poi archiviati nell'archivio di identità, come potrebbe in pratica un'autorità nazionale avviare una ricerca in questo archivio senza disporre degli stessi dati corrispondenti da inserire nella richiesta? Queste domande apparentemente tecniche rivelano seri questioni in ter-

mini di pertinenza dei dati utilizzati in relazione agli usi e agli scopi del trattamento perché soltanto i dati corrispondenti possono essere utilizzati per avviare una *query*, ma è impossibile per un individuo sapere se vi siano anche altri dati inclusi nelle banche dati di cui le autorità nazionali dispongono e che pertanto non possono essere rese interoperabili. Inoltre, questa complessa architettura rivela importanti carenze che potrebbero pregiudicare i diritti effettivi dei cittadini di paesi terzi. Può accadere infatti che i dati incompleti non siano utilizzati dalla stessa autorità che li ha inseriti nelle banche dati, ma da altri utenti, rispettando o meno le indicazioni fornite dalle autorità che inseriscono i dati nei database singoli (cosiddetti *data originators*) ma non necessariamente in modo trasparente. I dati personali integrati nelle banche dati dalle autorità nazionali possono diventare ulteriormente ricercabili e accessibili da parte delle agenzie europee (a condizione che siano stati presi accordi specifici con loro) o delle autorità nazionali di altri Stati membri che potrebbero utilizzare tali dati nel proprio contesto di attività.

L'interoperabilità dei sistemi informativi implica dunque non soltanto la piena disponibilità dei dati rilevanti ma anche interconnessioni tra le funzionalità delle componenti interoperabili operanti trasversalmente e contestualmente su basi di dati. Ciò non significa la creazione di "un enorme database in cui tutto è interconnesso", ma la capacità dei sistemi informativi di scambiare dati personali e di consentire la condivisione delle informazioni.

Grazie alla struttura istituzionale flessibile delle banche dati dell'UE (SIS II, VIS, Eurodac, EES, ETIAS, ECRIS-TCN), l'archiviazione e lo scambio di informazioni sono diventati un elemento essenziale della cooperazione europea, che può essere realizzato attraverso l'accesso ai dati. I flussi di dati personali integrati in un sistema informativo interoperabile modellano, da un lato, i diritti e gli interessi delle persone, in particolare dei cittadini di paesi terzi i cui dati personali saranno archiviati e ulteriormente trattati in modi interoperabili per molteplici scopi; dall'altro, il potere discrezionale delle autorità nel concedere l'accesso a tali dati.

I cittadini di paesi terzi sono spesso obbligati a consegnare i propri dati anche se hanno soltanto in mente di richiedere un visto o altri permessi/autorizzazioni. Non hanno altra scelta.

Va da sé che lo scopo perseguito dal framework sulla interoperabilità per affrontare la cosiddetta "frode di identità" richiede che l'identità personale sia costruita sulla base di informazioni frammentate che vengono condivise, trasferite, disaggregate e riaggregate in modo

*Nationals' Data or a Step Backwards in the Protection of Fundamental Rights?*, in V. Mitsilegas e N. Vavoula (a cura di), *Surveillance and Privacy in the Digital Age. European, Transatlantic and Global Perspectives*, Oxford, Hart Publishing, pp. 159-196.

<sup>27</sup> In senso più ampio si veda Ferraris V. (2020), *Il migrante datificato nei confini del futuro: senza potere di fronte a un oscuro potere?*, in S. Gozzo, C. Pennisi, V. Asero, R. Sampugnaro (a cura di), *Big Data e processi decisionali. Strumenti per l'analisi di decisioni giuridiche, politiche, economiche e sociali*, Egea, Roma, pp. 135-148.



parziale e stigmatizzante<sup>28</sup>. Ciò può compromettere gravemente i diritti dei cittadini di paesi terzi, i quali sono maggiormente colpiti dall'uso improprio dei dati. Inoltre, ciò può comportare una minore tutela dei loro diritti, in quanto essi non essendo cittadini europei non hanno automaticamente accesso alle corti nazionali ma soltanto a speciali forme di protezione internazionale. Tale conclusione appare sconcertante se si pensa che è esattamente ciò che l'interoperabilità dovrebbe mirare a evitare. In una configurazione così complessa nella quale si intrecciano molteplici livelli normativi e diversi interessi in gioco, l'interoperabilità svolge un ruolo cruciale nella riconfigurazione di un nuovo ordine geopolitico in tutta l'UE, che cerca di combinare strumenti formali e pratiche informali di condivisione delle informazioni tentando di evitare che si rimanga intrappolati in una terminologia tecnica e operativa che è ovviamente ambigua.

Il quadro normativo che regola i sistemi informativi interoperabili e le singole banche dati è ricco di indicazioni che suggeriscono l'opzione della indisponibilità dei dati. Tuttavia, il fulcro della condivisione delle informazioni è rappresentato dal significato che il diritto di accesso può assumere in modo diverso nel tempo e in cosa possono consistere specificamente le conseguenze che derivano dall'accesso ai dati e dal loro uso. Entrambi i regolamenti sull'interoperabilità impongono requisiti rigorosi per l'accesso all'archivio comune delle identità per l'identificazione da parte delle autorità di polizia e per l'individuazione di identità multiple da parte delle autorità preposte alla verifica manuale delle identità, nonché per l'accesso a più rilevatori di identità da parte di singole banche dati.

Come sottolineato dall'Agenzia per i diritti fondamentali a proposito dell'ambigua formulazione dei regolamenti sulla interoperabilità, il fatto che l'accesso ai dati debba avvenire in conformità con il profilo dell'utente e i diritti di accesso dipendano dalla ricerca originariamente avviata dal funzionario anziché dai risultati della ricerca mostra una enorme lacuna logica. Inoltre, qualora sia necessario l'autorità nazionale competente potrebbe avere accesso a informazioni aggiuntive oltre a quelle che è autorizzata a visualizzare. La formulazione poco chiara dell'articolo 9 potrebbe condurre dunque a interpretazioni diverse e alla sua attuazione in modo non conforme al principio della limitazione delle finalità dei dati contenuto nel Regolamento generale sui dati personali<sup>29</sup>.

Si tratta dunque di una struttura istituzionale flessibile che abilita i processi informativi a definire gli elementi della cooperazione: essa consiste nella raccolta e scambio di dati e nella loro interpretazione. Tuttavia, interoperabilità dei sistemi informativi non significa sistema centralizzato e allineato con priorità predefinite. Esistono infatti vari gradi di complessità: una varietà di agenzie e attori coinvolti; una condivisione bilaterale delle informazioni; la cooperazione tra agenzie; accordi di cooperazione esterna. Inoltre, la condivisione delle informazioni si combina con due strumenti che aggravano ulteriormente l'opacità e la segretezza: il principio del controllo della informazione da parte di chi la immette nel sistema (principio del controllo da parte dell'originatore dei dati); il principio di classificazione delle informazioni derivate.

Tutto ciò crea un processo di accumulazione tipico di ogni potere che consiste nel mantenere un vantaggio informativo al limite dei meccanismi tradizionali dell'amministrazione pubblica, senza limitazione di fatto delle finalità di trattamento dei dati e con il rischio di falsi risultati.

Interessante da ultimo notare che al momento la lista degli *high-risk systems* previsti dalla Commissione distingue "tecnologicamente" i sistemi utilizzati per contrasto ai crimini con quelli utilizzati nel campo dell'immigrazione, asilo e controllo delle frontiere, senza reale possibilità di separare a monte i flussi informativi che nella pratica rimangono spesso indistinti e confusi.

Questo costituisce soltanto un esempio per riflettere su come la classificazione dei sistemi ad alto rischio in relazione ai flussi informativi sia tutt'altro che operazione semplice e per di più attendibile. La gestione del rischio commisurata alle scelte di data governance sembrerebbe invece essere un'opzione realistica più aderente alla pratica del *trial & error* nonché calata in una realtà sociale che muta.

## CONCLUSIONI

Nelle riflessioni svolte si è tentato di delineare le caratteristiche principali del rapporto tra rischio, inteso come limite modulabile offerto dal diritto della intelligenza artificiale alla policy dell'intelligenza artificiale, e vulnerabilità, presentata come alterazione della capacità di controllo umano cognitivo e fattuale.

Se da un lato è intuibile, anche in base alle soluzioni offerte dalla proposta, forse la semplificazione concettuale eccessiva in cui l'Unione Europea è incorsa – ravvisando come contraltare della vulnerabilità la valutazione e gestione del rischio – di contro va apprezzato lo sfor-

<sup>28</sup> Pelizza A. (2019), *Processing Alterity, Enacting Europe. Migrant registration and identification as co-creation of individuals and politics*, in «Science, Technology and Human Values», 45(2): 262-288.

<sup>29</sup> Fra Opinion 1/18 (Interoperability), Interoperability and fundamental rights implications, [https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2018-opinion-01-2018-interoperability\\_en.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-01-2018-interoperability_en.pdf), 19.

zo volto a mettere in piedi una architettura sofisticata di classificazione e misure relative ai sistemi di intelligenza artificiale sulla base del rischio inaccettabile, che in fin dei conti si può immaginare come razionalità materiale del nostro futuro-presente.

Il caso studio dell'impatto della interoperabilità dei sistemi informativi europei sui diritti dei cittadini di paesi terzi è emblematico in quanto rappresenta un esempio di come la frammentarietà della storia identitaria, riflessa in dati frammentati, abbia un effetto di segmentazione della realtà che può dar luogo a decisioni errate.

La scelta di porre al centro dello sviluppo del mercato europeo e della strategia digitale l'individuo non come limite ma come alternativa razionale di mutamento e sviluppo sociale è probabilmente l'inedito europeo che con tutta la sua inevitabile retorica vale la pena esplorare nelle pratiche.

È tuttavia necessario riconoscere i luoghi nei quali si annidano le sacche di vuoto di sistema anche per comprendere esattamente a cosa ci si riferisce quando il regolamento parla di sorveglianza umana.

La prima macroscopica fallacia riguarda il concetto stesso di approccio antropocentrico.

Non si tratta certamente di un concetto di individualismo tradizionale nel quale l'individuo libero si pone al centro delle proprie scelte e si autodetermina dal punto di vista tecnologico<sup>30</sup>. Al più, abbiamo visto come all'individuo rimanga la possibilità di autodeterminarsi dal punto di vista informativo. Il punto è realisticamente quello di comprendere se un individuo singolo possa o meno esercitare realmente un pieno controllo di un sistema ad alto rischio. L'ambizione europea deve essere dunque coltivata nel senso di sviluppare una nuova idea di individualismo collettivo, cioè di quella individualità globale che nella propria identificazione con alcuni capitali del progetto di integrazione europea, come i valori dell'Unione e i diritti fondamentali, possa avere la possibilità di agire collettivamente.

Mi riferisco in particolare alla possibilità di contrastare gli standard contenuti nella documentazione tecnica predisposta dagli organismi notificati<sup>31</sup> e facenti parte di un elenco approvato dalla Commissione, che possono costituire un lasciapassare rispetto al quale è abbastanza inverosimile che il cittadino europeo tipo – per non parlare di soggetti vulnerabili, come ad esempio cittadini di paesi terzi – possa esercitare di fatto forme di controllo. La messa in atto di un sistema di gestione della qualità

dei dati, degli obblighi di redigere la documentazione tecnica prima dell'immissione nel mercato e di partecipare a una procedura di valutazione di conformità da parte dei fornitori dei servizi si risolve il più delle volte in un processo seppur complesso e stringente di certificazioni il cui contenuto – gli standard tecnici – è spesso coperto da proprietà intellettuale e comunque confidenziale e pertanto inaccessibile<sup>32</sup>.

Rispetto a tale scenario, la proposta europea non contempla rimedi giurisdizionali in capo agli individui né tanto meno azioni di classe. Non si tratta dunque soltanto di una questione di asimmetria informativa, bensì di deficit democratico ed esclusione dai processi decisionali di soggetti rispetto ai quali la previsione della sorveglianza umana (art. 14) appare un processo anch'esso standardizzato a intermittenza, sulla base di regole predisposte dai fornitori dei servizi.

La seconda questione è quella relativa ai sistemi a rischio minimo, tutti quelli cioè non inclusi nell'allegato III che tipizza i sistemi ad alto rischio, la cui gestione è sostanzialmente delegata alla *self-regulation* dei privati e che evidentemente può determinare situazioni di vulnerabilità che sfuggono al controllo.

Un timido compromesso è stato individuato nella proposta di regolamento nel considerando n. 41 tale per cui il fatto che un sistema sia classificato ad alto rischio non implica necessariamente e automaticamente la sua liceità e conformità rispetto a diversa normativa Europea e nazionale e che tutti i sistemi di intelligenza artificiale devono essere predisposti e utilizzati in conformità alla Carta Europea dei diritti fondamentali. Tuttavia, si tratta di un edulcorato di bilanciamento delle pratiche con il rispetto dei diritti fondamentali che viene fatto a monte dai privati e anch'esso certificato come *legal design* preconfezionato.

Insomma, la correlazione di rischio e vulnerabilità apre importanti prospettive, che potrebbero tuttavia rimanere soltanto prospettive, non eliminando peraltro un incremento dei costi a carico dei fornitori dei sistemi, se l'Europa non prende fino in fondo coscienza delle proprie scelte.

#### RIFERIMENTI BIBLIOGRAFICI

Catanzariti M. (2019) *Individuals or 'bare data'? Unowned Data for Interoperable Borders*, <https://migrationpolicycentre.eu/individuals-or-bare-data/>.

<sup>30</sup> Rodotà S. (1995 [2021]) *Tecnologie e diritti* (a cura di G. Alpa, M.R. Marella, G. Marini, G. Resta), il Mulino, Bologna.

<sup>31</sup> È definito organismo notificato un organismo di valutazione della conformità designato in conformità al presente regolamento e ad altre pertinenti normative di armonizzazione dell'Unione.

<sup>32</sup> Veale M. e Borgesius F.Z. (2021), *Demystifying the Draft EU Artificial Intelligence Act. Analyzing the good, the bad, and the unclear elements of the proposed approach*, in «Computer Law Review International», 4: 97-112. Si vedano gli artt. 17, 18, 30, 32 e 33 AI Act.



- Catanzariti M. (2021), *Etica "artificiale": un nuovo modello regolatorio?*, in «Ars Interpretandi», 1: 165-179.
- Ceri P. e Borgna P. (1996), *La tecnologia per il XXI° sec. Prospettive di sviluppo e rischi di esclusione*, Einaudi, Torino.
- Cohen J. (2019), *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press, Oxford.
- Dumbrava C. (2021), *Artificial Intelligence at EU Borders: Overview of Applications and Key Issues*, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRSIDA\(2021\)690706EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRSIDA(2021)690706EN.pdf), (last visited 10 September 2021).
- Ferraris, V. (2020), *Il migrante datificato nei confini del futuro: senza potere di fronte a un oscuro potere?*, in S. Gozzo, C. Pennisi, V. Asero, R. Sampugnaro (a cura di), *Big Data e processi decisionali. Strumenti per l'analisi di decisioni giuridiche, politiche, economiche e sociali*, Egea, Roma.
- Foucault M. (2016), *Il coraggio della verità. Il governo di sé e degli altri II. Corso al Collège de France (1984)*, Feltrinelli, Milano.
- Golia A., Teubner G. (2021), *Networked statehood: an institutionalised self-contradiction in the process of globalisation?*, in «Transnational Legal Theory», 1-37.
- Magatti M. (2009), *La libertà immaginaria. Le illusioni del capitalismo tecno-nichilista*, Feltrinelli, Milano.
- Malgieri G., Niklas J. (2020), *Vulnerable Data Subjects*, in «Computer Law & Security Review», 37: 1-22.
- Gallino L. (2007), *Tecnologia e democrazia. Conoscenze tecniche e scientifiche come beni pubblici*, Einaudi, Torino.
- Mantelero A. (2022), *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, Springer, The Hague.
- Pelizza A. (2019), *Processing Alterity, Enacting Europe. Migrant registration and identification as co-creation of individuals and polities*, in «Science, Technology and Human Values», 45(2): 262-288.
- Popitz H. (1990), *Fenomenologia del potere. Autorità, violenza, dominio, tecnica*, il Mulino, Bologna.
- Rodotà S. (1995 [2021]), *Tecnologie e diritti* (a cura di G. Alpa, M. R. Marella, G. Marini, G. Resta), il Mulino, Bologna.
- Rossi P. (2017), *Razionalismo occidentale e calcolabilità giuridica* in A. Carleo (a cura di), *Calcolabilità giuridica*, il Mulino, Bologna.
- S. Gozzo, C. Pennisi, V. Asero, R. Sampugnaro (2020) (a cura di), *Big Data e processi decisionali. Strumenti per l'analisi di decisioni giuridiche, politiche, economiche e sociali*, Egea, Roma.
- Vavoula N. (2021), *Interoperability of EU Information Systems in a "Panopticon" Union: A Leap Towards Maximised Use of Third-Country Nationals' Data or a Step Backwards in the Protection of Fundamental Rights?*, in V. Mitsilegas e N. Vavoula (a cura di), *Surveillance and Privacy in the Digital Age. European, Transatlantic and Global Perspectives*, Hart Publishing, Oxford.
- Veale M., Borgesius F.Z. (2021), *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, in «Computer Law Review International», 4: 97-112.
- Viljoen S. (2021-22), *A Relational Theory of Data Governance*, in «The Yale Law Journal», 131: 573-653.
- Zeno Zencovich V. (2017), *Ten Legal Perspectives on the "Big Data Revolution"*, Editoriale Scientifica, Napoli.
- Zuboff S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma.