

# Il diritto costituzionale e le sfide dell'innovazione tecnologica

<b>Sottotitolo:</b>	Atti del Convegno di Genova - 18-19 giugno 2021
<b>Autori:</b>	P. Costanzo, P. Magarò, L. Trucco (a cura di)
<b>ISBN:</b>	979-12-5976-279-5
<b>N. Pagine:</b>	504
<b>Anno Pubbl.:</b>	2020
<b>Collana:</b>	Collana del Gruppo di Pisa
<b>Numero:</b>	19
<b>Materia:</b>	Diritto costituzionale

## IL DIRITTO COSTITUZIONALE E LE SFIDE DELL'INNOVAZIONE TECNOLOGICA

Atti del Convegno di Genova  
18-19 giugno 2021



COLLANA DEL GRUPPO DI PISA

EDITORIALE  
SCIENTIFICA



Product ISBN: 979-12-5976-279-5

### 30,40 €

Base price 32,00 €

Discount 1,60 €

1



**Aggiungi al Carrello**



[? Ask a question about this product](#)

# I SISTEMI DI IDENTIFICAZIONE BIOMETRICA A DISTANZA: UN ESEMPIO PARADIGMATICO DELLE SFIDE LANCIATE DALLA TECNOLOGIA AL DIRITTO COSTITUZIONALE

di Giuseppe Mobilio

SOMMARIO: 1. Considerazioni introduttive. – 2. Le tecnologie biometriche di identificazione: peculiarità, potenzialità e pericolosità. – 3. Le difficoltà del diritto alle prese con queste tecnologie. – 4. Alcune conseguenze nell'impiego di tecnologie biometriche da parte dei pubblici poteri. – 5. I diritti fondamentali a rischio. – 6. L'esigenza di una regolamentazione giuridica all'altezza della sfida.

## 1. Considerazioni introduttive

Tra le tecnologie algoritmiche basate sull'intelligenza artificiale ve ne sono alcune che risultano paradigmatiche – riprendendo il titolo di questa iniziativa scientifica – per le sfide che l'innovazione tecnologica ha lanciato al diritto costituzionale. Si tratta dei sistemi di identificazione biometrica a distanza, che, non a caso, il più recente tentativo di disciplina a livello europeo sull'intelligenza artificiale, ossia la proposta di regolamento diffusa dalla Presidente della Commissione europea a fine aprile 2021<sup>1</sup>, inquadra tra quelle espressamente “proibite”, salvo che non vengano rispettate determinate condizioni.

L'obiettivo di questa breve nota è dar conto di come vi siano esempi di tecnologie in grado, alla prova dei fatti, di intercettare molteplici profili problematici evocati dalle Relazioni sin qui svolte, offrendo lo spunto per andare a fondo, e forse anche riconsiderare numerose categorie del diritto costituzionale<sup>2</sup>.

<sup>1</sup> Cfr. Proposal for a “Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts” (COM/2021/206 final), 21 aprile 2021.

<sup>2</sup> In generale, sull'impatto delle tecnologie algoritmiche digitali sulle categorie del diritto costituzionale, v. A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1, 2019, 63 ss.; C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Dir. pubb. comp. eur.*, f.s., 2019, 101 ss.; A. D'ALOIA, *Il diritto verso “il mondo nuovo”*. *Le sfide dell'Intelligenza Artificiale*, in ID. (a cura di), *Intelligenza artificiale e diritto*, Milano, 2020, 7 ss.; B. CARAVITA DI TORITTO, *Principi costituzionali*

## 2. Le tecnologie biometriche di identificazione: peculiarità, potenzialità e pericolosità

Per dare conto di quanto detto occorre innanzitutto chiarire preliminarmente cosa si intenda per sistemi di identificazione biometrica a distanza. Nello specifico, si tratta di tecnologie che consentono di identificare con esattezza una persona a partire da alcune sue caratteristiche biometriche uniche, quali i tratti fisici, come l'immagine del volto, oppure i tratti differenziali del suo comportamento, come il modo di camminare o il timbro della voce.

A differenza di quanto accade per altre caratteristiche biometriche, come il DNA, le impronte digitali o la struttura vascolare della retina, attraverso questi sistemi l'identificazione può avvenire a distanza, ossia senza alcun contatto fisico dell'interessato, ma semplicemente tramite l'elaborazione digitale di una immagine o del suono catturati da una fotocamera, da una videocamera a circuito chiuso o da un microfono anche molto lontani dall'interessato<sup>3</sup>. I dati così acquisiti vengono comparati con altri dati presenti in un *database* e già associati alla persona cui appartengono. Questa comparazione avviene in maniera automatizzata, tramite complessi algoritmi di intelligenza artificiale in grado di processare i dati (audio e video) acquisiti dal vivo per ricercare eventuali corrispondenze, permettendo così di risalire non solo alle generalità di un individuo, ma anche ad una serie di ulteriori informazioni ottenute tramite l'incrocio con altre banche dati o le informazioni presenti su internet. Il processo così sommariamente descritto avviene a grande velocità, senza che l'interessato se ne accorga o che debba manifestare alcun atteggiamento cooperativo, prescindendo potenzialmente dall'intervento di alcun essere umano<sup>4</sup>.

Queste tecnologie offrono una miriade di opportunità, delle quali solo di recente si sta acquisendo consapevolezza. Nel settore privato, ad esempio, gli operatori economici, le piattaforme del *web* e i *social network* vi fanno impiego per motivi di sicurezza, per proporre suggerimenti di acquisto o per ampliare il *network* di conoscenti. Nel settore pubblico il loro utilizzo è legato allo svolgimento di indagini penali o i controlli alle frontiere, alla

*e intelligenza artificiale*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 451 ss. Più in generale, sulle dinamiche di trasformazione del costituzionalismo in relazione alla dimensione tecnologica, cfr. P. COSTANZO, *Il fattore tecnologico e le trasformazioni del costituzionalismo*, in ASSOCIAZIONE ITALIANA DEI COSTITUZIONALISTI, *Costituzionalismo e globalizzazione*, Napoli, 2014, 43 ss.

<sup>3</sup> Cfr. E. LEARNED-MILLER, V. ORDÓÑEZ, J. MORGENSTERN, J. BUOLAMWINI, *Facial Recognition Technologies in the Wild: A Primer*, 29 maggio 2020, 8.

<sup>4</sup> Cfr. GARVIE ET AL., *The Perpetual Line-Up. Unregulated Police Face Recognition in America*, Georgetown Center on Privacy & Technology, 18 ottobre 2016, 16 ss.

prevenzione e alla garanzia della sicurezza pubblica, oppure per rendere le città sempre più *smart*. Di converso, quello che così si manifesta è un potere di sorveglianza sempre più pervasivo e ubiquitario, che può essere sfruttato anche per controllare, per tracciare e per manipolare singoli individui o interi gruppi di persone, perseguendo scopi tutt'altro che legittimi<sup>5</sup>. Non stupisce, quindi, che la già richiamata proposta di regolamento sull'IA abbia circondato di cautele l'utilizzo di queste tecnologie, soprattutto se realizzato da parte delle autorità pubbliche "in tempo reale", ovvero con una identificazione istantanea delle persone coinvolte; se disposto entro spazi pubblici, con la conseguenza di coinvolgere una quantità indefinibile di persone; se sfruttato per scopi di polizia. Allo scopo vengono indicati una serie di requisiti, finalità di impiego e obblighi di relativa autorizzazione che dovrebbero valere a circoscrivere i possibili abusi<sup>6</sup>.

Riprendendo una osservazione svolta da Carlo Colapietro nel corso di questo Convegno, l'uso di tecnologie di identificazione biometrica a distanza costituisce una sfida "per" i diritti, nel senso che possono rappresentare strumenti molto utili alla salvaguardia dei diritti fondamentali (si pensi alla repressione di reati gravi o legati al terrorismo), ma anche una sfida "ai" diritti, nel senso che sono in grado di incidere e di ledere diritti in maniera inimmaginata.

### 3. Le difficoltà del diritto alle prese con queste tecnologie

Un primo profilo da sottolineare in relazione a queste tecnologie innovative è la difficoltà del diritto ad offrire una regolamentazione che possa dirsi adeguata ed efficace, tanto da correre il rischio di andare incontro – prendendo in prestito un termine riferito alla stessa tecnologia e alla teoria economica – ad una vera e propria "*disruption*" che ne sancisca il superamento da parte di altre forme di regolazione imposte, ad esempio, dal mercato o dalla tecnica stessa<sup>7</sup>. Attualmente nel panorama europeo – a quanto consta – nessuno Stato ha adottato una disciplina giuridica di rango primario che si rivolga a questi strumenti. L'assenza di una normativa sul punto trae origine da una molteplicità di fattori, dei quali è sufficiente qui indicare i seguenti.

Un primo fattore di spiegazione è riconducibile ad una questione di "ritmo": mentre la tecnologia evolve esponenzialmente, il diritto segue dinamiche di produzione molto più lente, in una sorta di "desincronizzazione"

<sup>5</sup> Sul punto, basti rinviare a D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2002; P. PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Milano, 2020.

<sup>6</sup> V. in particolare l'art. 5 della proposta di "Artificial Intelligence Act" citata *retro* in nota 1.

<sup>7</sup> Sul punto, volendo, v. G. MOBILIO, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, in *BioLaw Journal*, 2, 2020, 401 ss.

tra il tempo umano e quello della tecnologia<sup>8</sup>. La ricerca e lo sviluppo nel settore dei sistemi di sorveglianza in parola sono ad appannaggio di operatori privati e, in particolare, dei c.d. *Big Tech*, ovvero quelle multinazionali che dispongono del *know how*, delle risorse e dei dati indispensabili per essere competitivi nel mercato globale. Questi soggetti hanno impresso all'innovazione un ritmo a dir poco impetuoso, detenendo un patrimonio conoscitivo cui i soggetti pubblici rimangono estranei. I legislatori, in questo momento, stanno ancora prendendo coscienza dei rischi insiti nella diffusione di questi strumenti, a fronte di una domanda di mercato in costante crescita e che si autoalimenta, imponendo così la creazione di tecnologie sempre più sofisticate e all'avanguardia, secondo quella che viene definita una nuova forma di "capitalismo della sorveglianza"<sup>9</sup>. Da questa condizione di fatto derivano due conseguenze che meritano qui di essere sottolineate.

Da una parte, sono gli operatori economici che decidono se, e a quali condizioni consentire l'impiego di queste tecnologie, con conseguenze immediate sulla protezione dei diritti. Si pensi solamente all'esempio della produzione e commercializzazione di occhiali "smart" che integrano tecnologie di riconoscimento facciale, in grado, ad uno sguardo, di identificare le persone e fornire informazioni su di loro; ipotesi inizialmente sospesa per i rischi cui i diritti e le libertà delle persone vengono esposti, ma oggetto di interesse sempre maggiore da parte del mercato<sup>10</sup>.

Dall'altra, i pubblici poteri che vogliono fare ricorso a questo tipo di tecnologie sono costretti ad affidarsi agli operatori privati. Si pensi a quanto accaduto durante l'emergenza pandemica da Covid-19 e alla circostanza che sistemi di identificazione biometrica, gestiti da soggetti privati, siano stati impiegati per misurare la temperatura delle persone tra la folla e tracciare coloro che risultano potenzialmente infetti<sup>11</sup>. Dal momento che questi strumenti sono in grado di raccogliere massivamente dati rilevanti sulle persone,

<sup>8</sup> L. ALEXANDRE, *La guerra delle intelligenze. Intelligenza artificiale contro intelligenza umana*, Torino, 2018, 51 ss.

<sup>9</sup> Si tratta delle americane "GAFA", ovvero (per limitarsi al settore del riconoscimento facciale) Google (e la collegata Alphabet), che ha sviluppato "FaceNet"; Amazon, e il suo "Rekognition"; Facebook, e il suo "Deepface"; Apple, e il suo "Face ID" (cui si può aggiungere Microsoft e IBM). Ma il discorso può essere esteso anche alle cinesi "BAT" (Baidu, Alibaba e Tencent, cui si può aggiungere Xiaomi). Il riferimento nel testo va alla già notissima elaborazione in S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019.

<sup>10</sup> Cfr. S. RODRIGUEZ, *Facebook is 'looking at' facial recognition technology for upcoming smart glasses, executive confirms*, in CNBC, 25 febbraio 2021.

<sup>11</sup> Cfr. M. VAN NATTA ET AL., *The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic*, in *Journal of Law and the Biosciences*, 7, 1, gennaio-giugno 2020.

concernenti ad esempio le condizioni di salute o le abitudini di spostamento, e che da tali dati è possibile estrarre ulteriori informazioni grazie alle tecniche di *big data analytics*, ne deriva come gli operatori a ciò preposti – in termini peraltro oligopolistici – si trovino in possesso di una risorsa conoscitiva preziosissima che opportunamente viene definita la “nuova valuta”<sup>12</sup> dell’economia digitale.

Ed è qui che il peso economico acquisito da questi grandi *players* assume anche un valore politico, nella misura in cui l’unica regolazione in vigore è quella che essi stessi hanno prodotto, compresa la scelta volontaria di non mettere a disposizione dei pubblici poteri certe tecnologie perché ritenute troppo pericolose<sup>13</sup>. Più in generale, inoltre, si tratta di un potere che si risolve nella possibilità di condizionare l’esercizio dei diritti fondamentali o la libera espressione di scelte democratiche<sup>14</sup>, finanche influenzare la decisione degli organi politici nel se, e come, adottare una regolazione su queste tecnologie<sup>15</sup>.

Un secondo elemento con cui il diritto deve fare i conti consta nella difficoltà – se non impossibilità – di ricondurre queste tecnologie alla giurisdizione di un unico ordinamento, fosse anche di tipo sovranazionale. I sistemi di identificazione biometrici offrono un esempio chiaro di come la tecnica costituisca un fattore di alimentazione dei processi di globalizzazione giuridica in corso<sup>16</sup>. Si consideri come i dati di cui si nutrono queste tecnologie algoritmiche, primi fra tutti le immagini, presentino un legame con il territorio fisico – a dir poco – labile. Il tentativo del diritto di “afferrare” il dato per regolarlo diviene quindi estremamente complicato, come emerge dallo sforzo compiuto a livello di UE tramite il regolamento (UE) 2016/679 sulla

<sup>12</sup> W.D. EGGERS, R. HAMILL, A. ALI, *Data as currency. Government’s role in facilitating the exchange*, in *Deloitte Review*, 13, 2013, 19 ss.

<sup>13</sup> R. HEILWEIL, *Big Tech Companies Back Away from Selling Facial Recognition Technology to Police. That’s Progress*, in *Vox*, 11 giugno 2020.

<sup>14</sup> Un potere che, come insegnano le recenti vicende che coinvolgono Facebook, consente di condizionare l’esercizio di libertà come quella di espressione – si pensi all’“Oversight Board”, nel delicato crinale tra controllo dei contenuti e censura – o diritti politici come quello di voto – si pensi allo scandalo di “Cambridge Analytica” e l’uso delle informazioni personali per manipolazioni di massa –; in tema, v. M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in *Rivista “Gruppo di Pisa”*, 2, 2021, 166 ss., e anche in questo volume.

<sup>15</sup> È il caso, ad esempio, della legislazione adottata nello Stato di Washington, criticata perché troppo poco rigida nel limitare l’uso di queste tecnologie da parte delle forze dell’ordine, il cui primo firmatario è il senatore Joe Nguyen, *program manager* della Microsoft; cfr. D. GERSHGORN, *A Microsoft Employee Literally Wrote Washington’s Facial Recognition Law*, in *OneZero*, 3 aprile 2020.

<sup>16</sup> Sulla quale, basti rinviare a C. NAPOLI, *Territorio, globalizzazione, spazi virtuali*, in *Rivista “Gruppo di Pisa”*, 2, 2021, 192 ss. e anche in questo volume.

protezione dei dati personali (c.d. GDPR)<sup>17</sup>. In questo scenario, la tutela giuridica è chiamata a farsi “dinamica”, ovvero a seguire i dati nella loro incessante circolazione, entro spazi oramai senza confini fisici<sup>18</sup>.

Ma si consideri anche come la scrittura dei *software* e la produzione dei componenti di questi sistemi sia realizzata da operatori provenienti dalle parti più disparate del mondo, così da rendere arduo stabilire a quale giurisdizione occorra fare riferimento per stabilire le regole da applicarsi. Una riprova si ha nelle difficoltà che anche a livello europeo si riscontrano nel riformare la disciplina sulla responsabilità civile derivante dal malfunzionamento di tecnologie algoritmiche di questo tipo<sup>19</sup>.

#### 4. Alcune conseguenze nell’impiego di tecnologie biometriche da parte dei pubblici poteri

L’impiego dei sistemi di identificazione biometrica a distanza da parte dei soggetti pubblici apre poi ad ulteriori scenari di questioni problematiche.

È il caso, innanzitutto, in cui la potenzialità di questi strumenti venga sfruttata dalle forze dell’ordine e dalla magistratura nel corso delle indagini penali. Al difficile rapporto tra autorità giudiziaria e tecnologie digitali, ben tratteggiato nella relazione di Erik Longo<sup>20</sup>, deve essere quindi ricollegato l’ulteriore tema della prova informatica (c.d. *digital evidence*, o *e-evidence*)<sup>21</sup> e, più da vicino, le condizioni alle quali il sapere tecnologico può trovare legittimamente ingresso nel procedimento penale<sup>22</sup>. Si tratta di un aspetto cruciale anche per la tutela dei diritti fondamentali all’interno del processo, affinché cioè la decisione giudiziaria non venga presa in segreto e vengano così garantiti il diritto di difesa dell’imputato (art. 24 Cost.) e la regola del contraddittorio nella formazione della prova (art. 111, c. 4, Cost.)<sup>23</sup>.

<sup>17</sup> Sul punto, volendo, v. G. MOBILIO, *L’intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *Federalismi.it*, 16, 2020, 285 ss., e i richiami ivi contenuti.

<sup>18</sup> Chiarissime le osservazioni in S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, 397 s.

<sup>19</sup> V. EUROPEAN COMMISSION, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, COM(2020) 64 final, 19 febbraio 2020.

<sup>20</sup> E. LONGO, *La giustizia nell’era digitale*, in questo volume.

<sup>21</sup> Cfr. S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020, 73 ss.

<sup>22</sup> Il riferimento va alle valutazioni che il giudice deve compiere per ammettere una prova di natura scientifica tramite il c.d. *Daubert test*, su cui v. P. TONINI, *La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Diritto penale e processo*, 11, 2011, 1341 ss.

<sup>23</sup> Cfr. V. MANES, *L’oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tec-*

In aggiunta, l'utilizzo di queste tecnologie da parte dei pubblici poteri, sia esso sistematico o meno, è in grado di incidere direttamente sull'esercizio di libertà legate alla partecipazione politica e sul tenore democratico di un ordinamento. Si pensi a quanto recentemente accaduto negli Stati Uniti, a partire dalla metà del 2020, a seguito delle proteste portate avanti dal movimento "Black Lives Matter" e all'intensificazione nell'uso delle tecnologie di identificazione biometrica da parte delle forze dell'ordine, molto criticato perché non improntato solamente a finalità repressive degli episodi di violenza<sup>24</sup>. Fino all'esempio paradigmatico del "Social Credit System" nella Repubblica Popolare Cinese, basato su un sistema di sorveglianza capillare, attraverso cui il governo è in grado di orientare il comportamento di massa di persone e imprese<sup>25</sup>.

## 5. I diritti fondamentali a rischio

Quanto riferito sin qui rende evidente come i sistemi di identificazione biometrica a distanza siano in grado di incidere su una molteplicità di diritti fondamentali. Sviluppando ulteriormente questo aspetto, si potrebbe sostenere come la cifra caratteristica di queste innovazioni tecnologiche stia proprio nella capacità di interferire trasversalmente sui diritti e le libertà, di singoli e di gruppi di persone, in termini e forme a loro volta innovative<sup>26</sup>. Sul punto, basti limitare il discorso ad alcuni profili che sono già stati toccati dalle relazioni.

I primi diritti a venire in gioco sono, senza dubbio, quelli legati alla privacy e alla riservatezza<sup>27</sup>. Questi ultimi, pur non essendo sovrapponibili, hanno in comune – come noto – una accezione negativa che vi ricollega il diritto ad escludere gli altri da una sfera che si vuole conservare nella propria intimità<sup>28</sup>. Al di là della loro esatta definizione, quel che è certo è che queste tecno-

*nocrazia*, in U. RUFFOLO (a cura di), *Intelligenza artificiale*, cit., 559 ss.

<sup>24</sup> Cfr. N. DAVIES, *US police are using facial recognition technology at protests - adding to systemic racism*, in *Business & Human Rights Resource Center*, 18 agosto 2020.

<sup>25</sup> Attraverso questo sistema a ciascun cittadino viene attribuito un numero identificativo e, grazie alla sorveglianza fisica e digitale continua, viene associato un punteggio che ne qualifica l'affidabilità e ne oggettiva la reputazione. Attraverso un sistema di benefici e sanzioni diviene possibile questa opera di orientamento di massa; più ampiamente, cfr. F. LIANG, V. DAS, N. KOSTYUK, M.M. HUSSAIN, *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in *Policy and Internet*, 4, 10, 2018, 415 ss.

<sup>26</sup> Sul punto, basti rinviare a G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, 57 ss.

<sup>27</sup> Cfr. S. SCAGLIARINI, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, in *Consulta Online*, 2, 2021, 491 ss.

<sup>28</sup> Cfr. M. TIMIANI, *Un contributo allo studio sul diritto alla riservatezza*, in *Studi parla-*



logie manifestano una spiccata capacità invasiva, nella misura in cui conferiscono a coloro che le utilizzano un potere di controllo e di tracciamento che, grazie ai potenti mezzi di analisi dei *big data*, può addirittura risolversi nella capacità di predire l'altrui comportamento e di manipolare le scelte assunte<sup>29</sup>.

Altri diritti interessati da queste tecnologie, poi, sono quelli legati alla protezione dei dati personali<sup>30</sup>. A questo proposito viene in gioco – come altrettanto noto – una componente positiva, intesa come diritto a mantenere un controllo sui propri dati, dando sostanza al concetto di “autodeterminazione informativa”<sup>31</sup>. La pretesa di mantenere questo controllo assume centralità nel contesto attuale, ove si assiste a quella che viene definita come la progressiva “datificazione” delle società, ovvero la quantificazione/conversione dei processi vitali in flussi di dati da elaborare tramite algoritmi e capace così di generare altre informazioni per una molteplicità di scopi<sup>32</sup>. I sistemi di identificazione biometrica, in particolare, contribuiscono a esercitare le diverse forme di c.d. “*dataveillance*” (forma contratta di *data-surveillance*), intesa come “impiego sistematico dei dati personali per indagare o monitorare le azioni o le comunicazioni di una o più persone”<sup>33</sup>. I diritti finalizzati alla protezione dei propri dati, così, acquisiscono una particolare valenza, poiché servono a resistere a queste forme di sorveglianza, offrendo così salvaguardia al libero sviluppo della personalità ed ai rapporti con gli altri consociati in un universo di relazioni *online*<sup>34</sup>.

Da ultimo non si può tacere uno degli aspetti che destano maggiore allarme, ovvero i fenomeni discriminatori che possono insorgere a seguito dell'impiego di tecnologie di identificazione biometrica; soprattutto quando le informazioni raccolte vengono poste a fondamento di decisioni che impattano su altri diritti fondamentali, a partire dalle limitazioni alla libertà personale.

Anche da tale punto di vista, queste tecnologie offrono una prospettiva privilegiata per comprendere i fattori che stanno alla base delle ipotesi di discriminazione nascenti dalla sottoposizione a sistemi algoritmici. Si fa ri-

*mentari e di politica costituzionale*, 2, 2012, 51 ss.; B.-J. KOOPS ET AL., *A Typology of Privacy*, in *University of Pennsylvania Journal of International Law*, 38, 2017, 483 ss.

<sup>29</sup> Più ampiamente, v. G. MOBILIO, *ult. op. cit.*, 68 ss.

<sup>30</sup> V. sempre S. SCAGLIARINI, *ult. op. cit.*, 492 ss.

<sup>31</sup> Cfr. S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, 108.

<sup>32</sup> Cfr. V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data: A Revolution that will Transform How We Live, Work and Think*, London, 2013, 154 ss.; C. SARRA, *Il mondo-dato. Saggi su datificazione e diritto*, Padova, 2019, spec. 29 ss.

<sup>33</sup> Cfr. R. CLARKE, *Information Technology and Dataveillance*, in *Communications of ACM*, 5, 31, maggio 1988, 499 (trad. nostra).

<sup>34</sup> S. CALZOLAIO, *Protezione dei dati personali*, in *Dig. Disc. Pubbl.*, Agg., 2017, 603.

ferimento ai c.d. *bias*, ovvero le “distorsioni” presenti all’interno dei sistemi informatici e responsabili dei fenomeni discriminatori.

Nell’ampia casistica delle “distorsioni” che possono affliggere tali sistemi<sup>35</sup>, basti qui soffermare l’attenzione su quelle che si insidiano principalmente all’interno dei dati impiegati per “allenare” gli algoritmi a identificare le persone. Gli algoritmi che operano automaticamente l’identificazione biometrica, infatti, possono veder compromessa la propria accuratezza e portare a risultati discriminatori se “allenati” con dati storici che riflettono pregiudizi impliciti, o se i dati campionati offrono una rappresentazione statisticamente distorta di gruppi rispetto al complesso della popolazione. Da questo punto di vista, le immagini impiegate – ad esempio – nel riconoscimento facciale dovrebbero rispecchiare la varietà dei tratti fenotipici delle persone, in relazione a sesso, età, origine etnica: maggiore è il “pluralismo” dei dati utilizzati, tendenzialmente maggiore sarà l’accuratezza del sistema nell’identificare le persone<sup>36</sup>. Recenti studi, tuttavia, dimostrano come le persone dalla pelle nera e le donne risultino fortemente sottorappresentati nella costruzione di questi *dataset*, al punto che le donne dalla pelle scura provocano tassi di errore nel riconoscimento facciale di gran lunga maggiori rispetto agli uomini dalla pelle chiara di origine caucasica<sup>37</sup>.

Il tema delle c.d. *algorithmic discriminations* è approfondito nella dottrina, ove spesso vengono sottolineati anche i limiti della legislazione vigente, europea e nazionale, nel contrasto a questi fenomeni, i quali difficilmente risultano riconducibili alle categorie tradizionali di discriminazione diretta e indiretta<sup>38</sup>. Ai fini del presente discorso si vuole sottolineare innanzitutto come le discriminazioni prodotte dalle tecnologie di identificazione biometrica originano proprio da alcuni degli stessi elementi che la Costituzione ritiene non dovrebbero fondare distinzioni irragionevoli, secondo la formu-

<sup>35</sup> In generale sul fenomeno dei *bias*, per la letteratura specialistica, anche informatica, v. S. BAROCAS, A.D. SELBST, *Big Data’s Disparate Impact*, in *California Law Review*, 104, 2016, 671 ss.; F.Z. BORGESIU, *Discrimination, artificial intelligence, and algorithmic decision-making*, Study for the Council of Europe, 2018.

<sup>36</sup> B.F. KLARE, M.J. BURGE, J.C. KLONTZ, R.W. VORDER BRUEGGE, A.K. JAIN, *Face recognition performance: Role of demographic information*, in *IEEE Transactions on Information Forensics and Security*, 7, 6, 2012, 1789 ss.

<sup>37</sup> Un tasso di errore sulle prime che può arrivare fino al 34,7%, rispetto ai secondi che originano un tasso di errore pari allo 0,8%; sul punto, v. J. BUOLAMWINI, T. GEBRU, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning*, 81, 2018, 77 ss. Una diversa tecnica di analisi viene impiegata invece in P. GROTH, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, NIST, dicembre 2019, 3 ss.

<sup>38</sup> Sul punto, basti rinviare a C. NARDOCCI, *Intelligenza artificiale e discriminazioni*, in questo volume.

lazione del principio di eguaglianza formale all'art. 3, c. 1, tra cui il sesso o la razza. Tuttavia, le discriminazioni possono andare a colpire persone maggiormente bisognose di tutela, risolvendosi in una forma di lesione dei diritti che discende direttamente dalla reale condizione soggettiva e sociale di svantaggio in cui si trova tale persona, in antitesi con gli obblighi di protezione della Repubblica derivanti dal principio di eguaglianza sostanziale all'art. 3, c. 2, Cost., che imporrebbe invece una particolare attenzione nei loro confronti e nei confronti della situazione di vulnerabilità in cui si trovano<sup>39</sup>.

È il caso dell'impiego di queste tecnologie, fra l'altro, verso i minori, gli anziani e le persone affette da disabilità. Anche rispetto a queste categorie di soggetti i sistemi di identificazione biometrica presentano seri problemi di accuratezza, dando luogo ad un tasso di falsi-positivi o falsi-negativi maggiore rispetto ad altri soggetti. In relazione all'età, infatti, occorre prestare la dovuta attenzione alla caducità temporale e all'alterazione degli elementi fisici usati per l'identificazione. Rispetto ai minori, in particolare, la rapida crescita e i cambiamenti nella fisionomia facciale del periodo evolutivo rendono estremamente difficoltosa l'identificazione basata sui tratti del volto<sup>40</sup>. In relazione alle disabilità, in aggiunta, occorre tener conto delle conseguenze derivanti da incidenti occorsi o sindromi specifiche che rendono del tutto atipico, e strettamente personale, lo stato morfologico e comportamentale di una persona<sup>41</sup>. Piuttosto che trascurare o accentuare la condizione di debolezza di questi soggetti, dunque, i pubblici poteri dovrebbero attivare tutti gli strumenti a disposizione per favorire l'impiego di queste tecnologie, in piena coerenza con gli indirizzi formulati dall'Unione europea, secondo una prospettiva autenticamente "antropocentrica"<sup>42</sup>, che sottometta cioè la tecnologia al servizio della persona e non lasci quest'ultima in balia della tecnologia e, soprattutto, di coloro che possono sfruttarla.

## 6. L'esigenza di una regolamentazione giuridica all'altezza della sfida

Quest'ultima considerazione offre lo spunto per rimarcare l'importanza della regolamentazione giuridica nel definire le condizioni per l'impiego di questi strumenti tecnologici, o nel porre un argine al relativo sviluppo che possa quanto meno indirizzare, se non dirigere, l'evoluzione esponenziale cui si è fatto sopra riferimento; sino alle ipotesi in cui, a mali estremi, il ricor-

<sup>39</sup> Più ampiamente, v. G. MOBILIO, *ult. op. cit.*, 108 ss.

<sup>40</sup> P. GROTH, M. NGAN, K. HANAOKA, *ult. op. cit.*, 2; FRA, *Under watchful eyes – biometrics, EU IT-systems and fundamental rights*, 2018, 90.

<sup>41</sup> Cfr. S. BYRNE-HABER, *Disability and AI-Bias*, in *Medium*, 11 luglio 2019.

<sup>42</sup> Così da ultimo EUROPEAN COMMISSION, *White Paper "On Artificial Intelligence - A European approach to excellence and trust"*, COM(2020) 65 final, 19 febbraio 2020.

so ad una certa tecnologia debba essere vietato, ad esempio, per perseguire certe finalità, se non *tout court*<sup>43</sup>. È quanto sta accadendo – come detto – a livello europeo con la bozza di regolamento sull’IA, nonostante le autorità a garanzia della protezione dei dati personali abbiano sollevato perplessità per come è stata impostata la disciplina sul punto, rimarcando la necessità di un approccio più restrittivo che giunga a bandire l’impiego delle tecnologie di identificazione biometrica negli spazi pubblici, oltre all’impiego di analoghe tecnologie in grado di categorizzare le persone in gruppi in base a fattori come l’etnia o il genere<sup>44</sup>. Di converso, negli Stati Uniti, ove notoriamente manca una disciplina a livello federale sulla protezione dei dati personali analoga al GDPR, si assiste nel più recente periodo all’adozione da parte dei singoli Stati, o addirittura delle singole città, di una disciplina rivolta variamente a questi sistemi, con la quale si stabiliscono moratorie o se ne vieta per un certo periodo di tempo l’uso da parte di determinati soggetti, siano essi privati o più spesso pubblici, come le forze di polizia, o per determinati impieghi, come all’interno delle scuole<sup>45</sup>. Affinché il diritto assolva a questo compito cruciale, tuttavia, occorre che vengano soddisfatte almeno due condizioni.

La prima – riprendendo uno spunto offerto, da ultimo, dalla prof.ssa De Minico – è che venga affermata con maggior vigore la presenza dello Stato – o meglio, dei vari livelli di governo coinvolti nella regolazione di questo tipo di tecnologie, a partire dall’Unione europea, ma anche da parte dei singoli Stati, nell’esercizio delle proprie prerogative sovrane in ambiti come la protezione dei diritti fondamentali o la tutela dell’ordine pubblico, o le Regioni e gli enti locali, a partire dagli interventi e le scelte *latu sensu* normative che sono chiamati a compiere<sup>46</sup>. Non è più ammissibile che la regolazione di queste tecnologie sia devoluta ad operatori privati, mossi prevalentemente da finalità lucrative, e che i regolatori pubblici si lascino “catturare” dal soggetto regolato, il quale riesce a imporre il proprio punto di vista<sup>47</sup>.

<sup>43</sup> Spunti sulla necessità che il diritto “guidi” e “orienti” la tecnologia anche in A. PAJNO ET AL., *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal*, 3, 2019, 215.

<sup>44</sup> Cfr. EDPB-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 giugno 2021.

<sup>45</sup> Per una panoramica al riguardo, v. J. SPIVACK, C. GARVIE, *A Taxonomy of Legislative Approaches to Face Recognition in the United States*, in A. KAK (a cura di), *Regulating Biometrics: Global Approaches and Urgent Questions*, AI Now Institute, settembre 2020, 89 ss.

<sup>46</sup> Si veda il d.l. 20 febbraio 2017, n. 14, convertito con modificazioni con la legge 18 aprile 2017, n. 48, che istituisce i c.d. “Patti per l’attuazione della sicurezza urbana”.

<sup>47</sup> F. SARPI, *La regolazione di domani. Come adeguare il processo normativo alle sfide dell’innovazione*, in *Rivista Italiana di Politiche Pubbliche*, 3, 2018, 439.

Questa esigenza consente di sottolineare la seconda condizione che deve realizzarsi, ovvero la necessità che le autorità pubbliche esercitino un certo grado di “fantasia” regolativa, dal momento che difficilmente la legge, di per sé sola, si dimostrerà in grado di veicolare una disciplina efficace ed effettiva nei confronti di queste tecnologie. Le fonti normative tradizionalmente concepite come interventi eteronomi che, seguendo una traiettoria *top-down*, si calano dall’alto per disciplinare un certo fenomeno, vantano una pretesa che è destinata a rivelarsi fallace. Le considerazioni svolte sopra circa il ruolo dei soggetti privati, la velocità con cui l’oggetto della disciplina si evolve o l’extra-territorialità della dimensione tecnologica, militano proprio in questo senso.

Con una certa dose di realismo occorre prendere atto del concorso di una serie di strumenti che già allo stato attuale, di fatto, offrono una cornice regolativa, per quanto disorganica, a tecnologie come quelle di identificazione biometrica e, più in generale, a quelle che si basano sull’intelligenza artificiale. Si pensi alle forme di autoregolazione spontanea formulata dagli stessi sviluppatori e fornitori di queste tecnologie<sup>48</sup>; le ipotesi di co-regolazione che i destinatari della disciplina concorrono ad adottare con il più diverso coinvolgimento del decisore pubblico<sup>49</sup>; gli standard, o norme tecniche, elaborati da organismi di standardizzazione, a livello internazionale o nazionale, allo scopo di garantire, ad esempio, la qualità dei dati processati e l’interoperabilità dei sistemi<sup>50</sup>; lo stesso *design* con cui gli algoritmi e i sistemi di identificazione biometrica vengono concepiti e realizzati, sfruttando la valenza regolativa che il codice esprime e la sua attitudine a inverare le norme giuridiche e preservare i diritti alla cui tutela esse sono preposte<sup>51</sup>; l’universo della *soft law* e le diverse forme che essa può assumere, dagli atti delle istituzioni dell’UE sino alle decisioni delle autorità amministrative indipendenti<sup>52</sup>. L’aspirazione cui il diritto può ambire è quella di coniugare l’adozione di regole e principi cogenti, la cui indispensabilità non può essere messa in discussione, con una

<sup>48</sup> Spunti su queste forme di *self-regulation*, e sui relativi limiti, in S. NAKAR, D. GREENBAUM, *Now you see me. Now you still do: facial recognition technology and the growing lack of privacy*, in *Boston University Journal of Science & Technology Law*, 23, 2017, 102 ss.

<sup>49</sup> I “codici di condotta” preposti alla protezione dei dati personali ne sono un chiaro esempio; sul punto, v. A.R. POPOLI, *Codici di condotta e certificazioni*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, Bologna, 2019, 546 ss.

<sup>50</sup> In generale sul punto, v. A. IANNUZZI, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Napoli, 2018, 31 ss.; C. SCOTT, *Standard-Setting in Regulatory Regimes*, in M. CAVE, R. BALDWIN, M. LODGE (a cura di), *The Oxford Handbook on Regulation*, Oxford, 2010, 104 ss.

<sup>51</sup> Imprescindibile il riferimento a L. LESSIG, *Code and Other Laws of Cyberspace*, New York, 1999.

<sup>52</sup> In generale, si veda la panoramica offerta in E. BUCALO, *Autorità indipendenti e soft law. Forme, contenuti, limiti e tutele*, Torino, 2018.

combinazione di questi strumenti regolativi atta ad indirizzarli verso la protezione di valori e interessi ritenuti meritevoli di tutela, anche nell'ottica dei rischi cui concretamente l'impiego di queste tecnologie può esporre, misurati sulla base di tecniche di valutazione di impatto che vengono valorizzate molto anche dalla più volte citata bozza di regolamento europeo sull'IA<sup>53</sup>.

Le sfide che le nuove tecnologie algoritmiche lanciano al diritto costituzionale sono molteplici e impegnative, a partire – come qui solamente accennato – dalle insidie nei confronti dei diritti fondamentali e la necessità di immaginare nuove forme di tutela, dalle forme di produzione normativa cui fare ricorso, dal rapporto fra regolatori e regolati: quella che si profila è forse una nuova stagione per il costituzionalismo<sup>54</sup>, con la quale siamo chiamati a ripensare certe categorie affinché la tecnologia conservi la sua valenza strumentale, o comunque cooperativa nei confronti dell'essere umano, senza che essa, e chi ne fa uso, possano prendere il sopravvento.

<sup>53</sup> Più approfonditamente sul punto, v. G. MOBILIO, *ult. op. cit.*, 287 ss.

<sup>54</sup> Cfr. A. SIMONCINI, *ult. op. cit.*, 89.