CONSULTA ONLINE
PERIODICO TELEMATICO ISSN 1971-9892

2021 FASC. III

(ESTRATTO)

GIUSEPPE MOBILIO

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

10 SETTEMBRE 2021

IDEATORE E DIRETTORE RESPONSABILE: PROF. PASQUALE COSTANZO

Giuseppe Mobilio

I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale[*] [**]

ABSTRACT: ***The essay deals with the legal problems arising from the widespread diffusion of remote biometric identification systems. These unparalleled technologies, based on artificial intelligence, are capable to involve some of the principal challenges that digital algorithmic technologies are posing to contemporary constitutionalism. Starting from the attempt of the most recent proposal of European regulation to dedicate more stringent rules to this issue, the analysis focuses on the difficulties of legal rules to regulate these instruments of surveillance and the overall threats to fundamental rights.***

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[1], 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[2].

---

[*] *Contributo pubblicato ai sensi dell'art. 3, comma 13, del regolamento della Rivista.*

[**] *Il contributo riprende il contenuto dell'intervento svolto in occasione del Convegno annuale dell'Associazione Gruppo di Pisa "*Il diritto costituzionale e le sfide dell'innovazione tecnologica*", 18-19 giugno 2021, la cui versione di sintesi è in corso di pubblicazione negli Atti del Convegno stesso.*

[1] 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, in particolare art. 5. Su questa proposta, v. L. FLORIDI, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Philosophy & Technology*, 2, 2021; M. VEALE – F.Z. BORGESIUS, *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, 2021; M. EBERS, *Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in L.A. Dimatteo, M. Cannarsa, C. Poncibò (a cura di), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge University Press, Cambridge, 2022.

[2] 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*, FrancoAngeli, Milano, 2020, 7 ss.; B. CARAVITA DI TORITTO, *Principi costituzionali e intelligenza artificiale*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, GFL, 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*, Jovene, Napoli, 2014, 43 ss., e più di recente ID., *Lo "Stato digitale": considerazioni introduttive*, disponibile nella versione provvisoria sul sito dell'Associazione "Gruppo di Pisa" con specifico riguardo ai poteri dello Stato.

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

Per dar 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[3]. 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[4].

Questo tipo di 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 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[5]. 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[6].

---

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

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

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

[6] Si parla al riguardo di uno "strettamente necessario" per finalità tassative quali: la ricerca di specifiche vittime potenziali di crimini, compresi i minori scomparsi; la prevenzione di specifiche, significative e imminenti minacce alla vita o alla sicurezza fisica di persone o determinate da attacchi terroristici; le indagini nei confronti di autori o sospettati di crimini riconducibili alla disciplina sul mandato di arresto europeo, per i reati nei confronti dei quali la disciplina statale prevede una pena massima almeno di tre anni. In questi casi, l'uso di sistemi di identificazione biometrica deve tener conto della natura della situazione, in particolare della serietà, probabilità e il livello di danno provocato dal mancato utilizzo di questi sistemi, oltre che delle conseguenze del loro impiego in termini di impatto sui diritti e sulle libertà, sempre rispetto alla serietà, probabilità e livello di danno provocato. Parimenti occorre rispettare le misure di salvaguardia ritenute necessarie e proporzionate e le condizioni stabilite per l'uso, con particolare riguardo alle limitazioni temporali, geografiche e personali. Per il relativo impiego sarà anche necessaria l'autorizzazione dell'autorità giudiziaria o di un'autorità amministrativa indipendente statale, salvo che una situazione d'urgenza possa giustificare la convalida

Come già osservato[7], 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[8].

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[9]. 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 è riconducibile ad una questione di "ritmo": mentre la tecnologia evolve esponenzialmente, il diritto segue dinamiche e processi di produzione molto più lenti, in una sorta di "desincronizzazione" tra il tempo umano e quello della tecnologia[10]. 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, stano 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"[11]. 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[12].

---

successiva. Tale autorizzazione può avvenire solamente sulla base di prove oggettive o l'indicazione chiara che l'impiego di tali tecnologie sia necessario e proporzionato per il perseguimento delle finalità sopra indicate. Gli Stati potranno stabilire restrizioni all'uso di queste tecnologie, salvo comunque stabilire regole dettagliate concernenti la sopra citata autorizzazione e le finalità sopra indicate rispetto alle quali le autorità competenti saranno autorizzate ad impiegare tali strumenti. Cfr. art. 5 della proposta di "Artificial Intelligence Act" citata *retro* in nota 1 (traduzione nostra).

[7] Da C. Colapietro nel corso del Convegno annuale dell'Associazione Gruppo di Pisa "*Il diritto costituzionale e le sfide dell'innovazione tecnologica*", cit.

[8] ... o solo paventata nei classici della letteratura e del cinema, o dalle più recenti serie televisive.

[9] 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.

[10] L. ALEXANDRE, *La guerra delle intelligenze*, cit., 51 ss.

[11] 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 teso va alla già notissima elaborazione in S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma, 2019.

[12] Cfr. S. RODRIGUEZ, *Facebook is 'looking at' facial recognition technology for upcoming smart glasses, executive confirms*, in CNBC, 25 febbraio 2021.

Dall'altra, i pubblici poteri che vogliano 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, identificare coloro che non indossano la mascherina e tracciare coloro che risultano potenzialmente infetti[13]. Dal momento che questi strumenti sono in grado di raccogliere massivamente dati rilevanti sulle persone, concernenti ad esempio le condizioni di salute o le abitudini di spostamento, e che da tali dati è possibile estrarre ulteriori informazioni, secondo le 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 che opportunamente è stata definita, in termini generali, come la "nuova valuta"[14] 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[15]. 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[16], finanche influenzare la decisione degli organi politici nel se, e come, adottare una regolazione su queste tecnologie[17].

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[18]. 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. Ne costituiscono una riprova l'acquisizione massiva di tali dati, favorita dalla enorme diffusione dei dispositivi di rilevamento sopra richiamati; la loro acquisizione indiretta, tramite il serbatoio interminabile costituito dal web e, in particolare, dai *social network*; le possibili forme di elaborazione e trasformazione, tramite algoritmi che operano su macchine fisiche o direttamente nel mondo virtuale; la capacità quasi illimitata di conservazione, in *database* localizzabili o su *cloud*; tutti elementi che rendono estremamente complicato il tentativo del diritto di "afferrare" il dato per regolarlo, come emerge dallo sforzo compiuto a livello di UE tramite il regolamento (UE) 2016/679 sulla protezione dei dati personali (c.d. GDPR)[19]. 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[20].

---

[13] 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,

[14] W.D. EGGERS, R. HAMILL, A. ALI, *Data as currency. Government's role in facilitating the exchange*, in *Deloitte Review*, 13, 2013, 19 ss.

[15] R. HEILWEIL, *Big Tech Companies Back Away from Selling Facial Recognition Technology to Police. That's Progress*, in *Vox*, 11 giugno 2020.

[16] Un potere che consente di condizionare l'esercizio di libertà come quella di espressione, secondo quanto insegnano le recenti vicende che coinvolgono *social network* come Facebook e l'esperienza del suo "Oversight Board", nel delicato crinale tra controllo dei contenuti e censura, o diritti politici come quello di voto, come emerso dallo scandalo di "Cambridge Analytica" e nell'uso delle informazioni personali per manipolazioni di massa; in tema, v. M. BETSU, *Poteri pubblici e poteri privati nel mondo digitale*, in *Rivista del "Gruppo di Pisa"*, 2, 2021, 166 ss.

[17] È il caso, ad esempio, della legislazione adottata nello Stato di Washington (su cui v. *infra* in nota 53), 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.

[18] Sulla quale, basti rinviare a C. NAPOLI, *Territorio, globalizzazione, spazi virtuali*, in *Rivista del "Gruppo di Pisa"*, 2, 2021, 192 ss.

[19] 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.

[20] Chiarissime e acute le osservazioni in S. RODOTÀ, *Il diritto di avere diritti*, cit., 397 s., riprese anche da C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano,

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 cui fare riferimento. Una riprova di questa realtà 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 questi tipo, allo scopo di individuare il soggetto cui imputare un eventuale danno[21].

4. *Alcune conseguen.*

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 le 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[22], deve essere quindi ricollegato l'ulteriore tema della prova informatica (c.d. *digital evidence*, o *e-evidence*)[23] e, più da vicino, le condizioni alle quali il sapere tecnologico può trovare legittimamente ingresso nel procedimento penale[24]. 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.)[25].

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[26]; oppure alle proteste che nel

---

C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017, 87.

[21] In dottrina, v. G. GUERRA, *La sicurezza degli artefatti robotici in prospettiva comparatistica. Dal cambiamento tecnologico all'adattamento giuridico*, il Mulino, Bologna, 2018; G. PASSAGNOLI, *Il diritto civile al tempo dell'intelligenza artificiale: spunti per una problematizzazione*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., 71. A livello di indirizzi elaborate dale istituzioni europee, v. EUROPEAN PARLIAMENT, *Resolution with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)), 16 febbraio 2017, e, più di recente e direttamente sul punto, 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.

[22] E. LONGO, *La giustizia nell'era digitale*, disponibile nella versione provvisoria sul sito dell'Associazione "Gruppo di Pisa".

[23] Per un'analisi processual-penalistica nel nostro ordinamento, v. M. PITTIRUTI, Digital evidence *e procedimento penale*, Giappichelli, Torino, 2017. Sul contesto europeo, v. B. JERMAN BLAŽIČ, T. KLOBUČAR, *Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society*, in *Information & Communications Technology Law*, 29, 1, 2020, 66 ss.

[24] Il riferimento va alle valutazioni che il giudice deve compiere per ammettere una prova di natura scientifica tramite il c.d. *Daubert test*, elaborato dalla giurisprudenza statunitense a partire dal 1993 e accolto nell'ordinamento italiano con gli indirizzi giurisprudenziali inaugurati da Cass., Sez. I, 21 maggio 2008, n. 31456, e da Cass., Sez. IV, 17 settembre 2010, n. 43786. In dottrina sul punto, 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.

[25] Cfr. V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo (a cura di), *Intelligenza artificiale*, cit., 559 ss.; A. PAJNO, *Intelligenza artificiale e sistema di tutela giurisdizionale*, in *Astrid Rassegna*, 3, 2020, 8 s.

[26] 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.

2019 sono divampate nel territorio di Hong Kong, in occasione dell'adozione delle nuove misure legislative sull'estradizione, e a come l'uso di queste tecnologie abbia indotto i manifestanti a coprire i propri volti con maschere o ombrelli, divenuti poi il simbolo della protesa[27]. 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[28].

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[29]. 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[30]. Quest'ultima – come noto – può essere intesa essenzialmente nella sua accezione negativa, acquisita sin dalle sue origini nell'ordinamento statunitense, come diritto ad escludere gli altri da una sfera che si vuole conservare nella propria intimità, sia essa psichica, fisica, o relazionale[31]. A questo diritto, che nel tempo ha acquisito contenuti multiformi e, invero, piuttosto evanescenti, potrebbe accostarsi quello che nel nostro ordinamento è chiamato diritto alla riservatezza, la cui portata risulta invece più ridotta, seppur non esattamente circoscritta[32]. Al di là della definizione esatta dei relativi contenuti, quel che è certo è che queste tecnologie manifestano una spiccata capacità di invaderne le rispettive sfere, 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[33].

Altri diritti interessati da queste tecnologie, poi, sono quelli legati alla protezione dei dati personali[34]. A questo proposito, se alla privacy viene riconosciuta una connotazione negativa, la protezione dei propri dati – come altrettanto noto – viene riconnessa ad una componente positiva, intesa come diritto a mantenere un controllo sull'insieme dei dati che costituisce la proiezione della propria persona nella società dell'informazione, dando sostanza al concetto di "autodeterminazione informativa"[35]. 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

---

[27] B. SCHMIDT, *Hong Kong Police Already Have AI Tech That Can Recognize Faces*, in Bloomberg, 22 ottobre 2019.

[28] 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, legato ai servizi pubblici o alla concessione di finanziamenti, 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.

[29] Sul punto, basti rinviare a G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., 57 ss.

[30] Cfr. S. SCAGLIARINI, *La tutela della* privacy *e dell'identità personale nel quadro dell'evoluzione tecnologica*, in questa *Rivista* 2021/II, 491 ss.

[31] Cfr. B.-J. KOOPS ET AL., *A Typology of Privacy*, in *University of Pennsylvania Journal of International Law*, 38, 2017, 483 ss.

[32] M. TIMIANI, *Un contributo allo studio sul diritto alla riservatezza*, in *Studi parlamentari e di politica costituzionale*, 2, 2012, 51 ss.; S. SCAGLIARINI, *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Aracne, Roma, 2013, 43 ss.

[33] Più ampiamente, v. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., 68 ss.

[34] Cfr. S. SCAGLIARINI, *La tutela della* privacy *e dell'identità personale nel quadro dell'evoluzione tecnologica*, cit., 492 ss.

[35] Cfr. S. RODOTÀ, *Tecnologie e diritti*, il Mulino, Bologna, 1995, 108. Più in generale, v. anche L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale Scientifica, Napoli, 2016, spec. 96 ss.

quantificazione/conversione dei processi vitali in flussi di dati da elaborare tramite algoritmi e generare così altre informazioni per una molteplicità di scopi[36]. 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"[37]. I diritti finalizzati alla protezione dei propri dati, così, acquisiscono una particolare valenza, poiché servono a resistere a queste forme di controllo e limitarne gli impieghi, pur legittimi, offrendo così salvaguardia al libero sviluppo della personalità ed ai rapporti con gli altri consociati in un universo di relazioni *online*[38].

In stretta connessione con i diritti fin qui richiamati vi è quello all'identità personale – considerabile come il «diritto ad essere sé stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo»[39] – e quello legato alla proiezione del sé nel mondo virtuale, ovvero l'identità digitale[40]. Si è osservato come la rete, in ragione soprattutto del processo di datificazione sopra menzionato, è in grado di operare una frammentazione e successiva ricomposizione della personalità di un individuo, offrendo più rappresentazioni che costituiscono proiezioni parziali e legate a contesti specifici, e «proprio per questo motivo facilmente non (del tutto) veritiere e pertanto meritevoli di formare oggetto di tutela»[41].

Le tecnologie di identificazione biometrica sono in grado di favorire enormemente questi processi di frammentazione, nella misura in cui sono in grado di "leggere" i tratti intrinsecamente unici delle persone e trasformarli in dati. In questo caso l'interferenza con il diritto all'identità digitale non si verifica tanto nell'attività di identificazione in senso stretto, quanto soprattutto nell'estrazione dai dati biometrici delle ulteriori informazioni che posso ricavarsi – legate, ad esempio, al sesso, l'etnia, l'età –, oppure all'attività di controllo e tracciamento che così diviene possibile – in termini, ad esempio, di abitudini o preferenze –. Queste informazioni possono essere impiegate per realizzare una massiccia opera di categorizzazione e profilazione delle persone[42]. Il singolo individuo viene così ricondotto all'interno di gruppi (c.d. *clusters*) accomunati da simili elementi informativi e, per ciò stesso, diviene oggetto di decisioni che si attagliano a quello specifico profilo o categoria, prescindendo completamente dalla sua individualità, in coerenza con il sottolineato processo di frammentazione della propria identità[43].

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 sotto questo 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 riferimento ai c.d. *bias*, ovvero le "distorsioni" presenti all'interno dei sistemi informatici e responsabili dei fenomeni discriminatori.

---

[36] Cfr. V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data: A Revolution that will Transform How We Live, Work and Think*, John Murray, London, 2013, 154 ss.; C. SARRA, *Il mondo-dato. Saggi su datificazione e diritto*, Cleup, Padova, 2019, spec. 29 ss.

[37] Cfr. R. CLARKE, *Information Technology and Dataveillance*, in *Communications of ACM*, 5, 31, maggio 1988, 499 (trad. nostra).

[38] S. CALZOLAIO, *Protezione dei dati personali*, cit., 603.

[39] Riprendendo Corte cost., sent. n. 13/1994, 5.1 cons. dir. Più ampiamente, v. G. FINOCCHIARO, *Identità personale (diritto alla)*, in *Dig. disc. priv., sez. civ.*, Agg. V, 2010, 721 ss.

[40] Sul punto, v. ampiamente I. TARDIA, *L'identità digitale tra memoria ed oblio*, ESI, Napoli, 2017, spec. 66 ss.

[41] Cfr. S. SCAGLIARINI, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, cit., 496 ss.

[42] Cfr. M. HILDEBRANDT, *Defining Profiling: A New Type of Knowledge?* in M. Hildebrandt, S. Gutwirth (a cura di), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008, 17 ss.; F. LAGIOIA, G. SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *Federalismi.it*, 11, 2020, 89 ss.

[43] V. ancora G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., 60 ss.

Nell'ampia casistica delle "distorsioni" che possono affliggere tali sistemi[44], basti qui soffermare l'attenzione su quelle che si insidiano principalmente all'interno dei dati impiegati per "allenare" gli algoritmi a identificare le persone (*training set*). 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[45]. Recenti studi, tuttavia, dimostrano come le persone dalla pelle nera e le donne risultino fortemente sottorappresentati nella costruzione dei *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[46].

Il tema delle c.d. *alghoritmic discriminations* è ben 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[47]. 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 formulazione 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, comma 2, Cost., che imporrebbe invece una particolare attenzione nei loro confronti e nei confronti della situazione di vulnerabilità in cui si trovano[48].

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[49]. In

---

[44] In generale sul fenomeno dei *bias* – che possono riguardare i *training set*, o i dati processati per assumere le singole decisioni, o ancora il modo con cui l'algoritmo viene progettato e realizzato – 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.; M. VEALE, R. BINNS, *Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data*, in *Big Data & Society*, 4, 2017; J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YU, *Accountable Algorithms*, in *University of Pennsylvania Law Review*, 165, 2017, 633 ss.; F.Z. BORGESIUS, *Discrimination, artificial intelligence, and algorithmic decision-making*, Study for the Council of Europe, 2018.

[45] 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.

[46] 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.; C.M. COOK, J.J. HOWARD, Y.B. SIROTIN, J.L. TIPTON, A.R. VEMURY, *Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems*, in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 1, 1, 2018, 32 ss. Una diversa tecnica di analisi viene impiegata invece in P. GROTHER, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, cit., 3 ss.

[47] Sul punto, basti rinviarsi a C. NARDOCCI, *Intelligenza artificiale e discriminazioni*, disponibile nella versione provvisoria sul sito dell'Associazione "Gruppo di Pisa".

[48] Più ampiamente, v. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., 108 ss.

[49] P. GROTHER, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, cit., 2. Si osserva in FRA, *Under watchful eyes – biometrics, EU IT-systems and fundamental rights*, cit., 90, che per

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[50]. 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"[51], 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 ricorso ad una certa tecnologia debba essere vietato, ad esempio, per perseguire certe finalità, se non *tout court*[52]. 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[53]. 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[54]. 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

---

compromettere l'accuratezza del riconoscimento è sufficiente che le immagini facciali registrate in gioventù vengano confrontate con immagini dello stesso soggetto dopo che siano trascorsi solamente cinque anni. Per questo, più in generale, si è verificato come lo stato attuale della tecnologia renda meno affidabile l'analisi di immagini di bambini al di sotto dei tredici anni.

[50] Cfr. S. BYRNE-HABER, *Disability and AI-Bias,* in *Medium*, 11 luglio 2019.

[51] Così a partire da EUROPEAN COMMISSION, *Communication "Artificial Intelligence for Europe"*, COM(2018) 237 final, 25 aprile 2018, secondo una prospettiva sviluppata poi in ID., *Communication "Building Trust in Human-Centric Artificial Intelligence"*, COM(2019) 168 final, 8 aprile 2019, e ID., *White Paper "On Artificial Intelligence - A European approach to excellence and trust"*, COM(2020) 65 final, 19 febbraio 2020.

[52] 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.

[53] 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.

[54] Lo Stato di Washington è stato il primo ad adottare una legislazione organica "Concerning the use of facial recognition services" da parte delle autorità pubbliche, comprese le forze di polizia, firmata dal Governatore il 31 marzo 2020, che produce effetti a partire del luglio 2021, mentre il 17 giugno il Maine ha approvato "An Act To Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials'", che entrerà in vigore il 1 ottobre 2021. Lo Stato di New York ha invece disposto una sospensione con riguardo all'impiego negli istituti scolastici (*Governor Cuomo Signs Legislation Suspending Use and Directing Study of Facial Recognition Technology in Schools*, in *Urban CNY*, 22 dicembre 2020), mentre la California l'8 ottobre 2019 aveva già deciso una sospensione nei confronti delle forze dell'ordine. La prima città che, dal maggio 2019, ha approvato il divieto per le forze dell'ordine di ricorrere a tali tecnologie è stata San Francisco.

singoli Stati, nell'esercizio delle proprie prerogative sovrane in ambiti come la protezione dei dati personali 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[55]. 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[56].

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 efficacie 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'extraterritorialità 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[57]; le ipotesi di co-regolazione che i destinatari della disciplina concorrono ad adottare con il più diverso coinvolgimento del decisore pubblico[58]; gli standard, o norme tecniche, elaborati da organismi di standardizzazione tecnica, a livello internazionale o nazionale, allo scopo di garantire, ad esempio, la qualità dei dati processati e l'interoperabilità dei sistemi[59]; 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[60]; 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[61]. 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

[55] 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", sottoscritti tra il prefetto ed il sindaco, attraverso cui individuare interventi sulla sicurezza urbana, per obiettivi, tra l'altro, quali prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria anche «attraverso l'installazione di sistemi di videosorveglianza» (art. 5, c. 2, lett. a). Nell'ambito di tali patti, oltre che degli accordi conclusi tra Stato e Regioni per la promozione della sicurezza integrata ai sensi dell'art. 3, possono essere individuati specifici obiettivi per l'incremento dei servizi di controllo del territorio e per la sua valorizzazione, comprensivi anche di progetti «per la messa in opera a carico di privati di sistemi di sorveglianza tecnologicamente avanzati, dotati di software di analisi video per il monitoraggio attivo con invio di allarmi automatici a centrali delle forze di polizia o di istituti di vigilanza privata convenzionati» (art. 7, comma 1-*bis*).

[56] F. SARPI, *La regolazione di domani. Come adeguare il processo normativo alle sfide dell'innovazione*, in *Rivista Italiana di Politiche Pubbliche*, 3, 2018, 439.

[57] 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*, cit., 102 ss.

[58] I "codici di condotta" preposti alla protezione dei dati personali ne sono un chiaro esempio; sul punto, v. D. HIRSCH, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, in Seattle University Law Review, 34, 2011, 439 ss.; A.R. POPOLI, *Codici di condotta e certificazioni*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, cit., 546 ss.

[59] In generale sul punto, v. A. IANNUZZI, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, 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 University Press, Oxford, 2010, 104 ss.

[60] Imprescindibile il riferimento a L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999. In tema v. almeno R. Brownsword, K. Yeung (a cura di), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Hart Publishing, Oxford, 2008; M. HILDEBRANDT, *Smart technologies and the End(s) of Law. Novel Entanglements of Law and Technology*, Edward Elgar, Cheltenham, 2015.

[61] In generale, si veda la panoramica offerta in E. MOSTACCI, *La* soft law *nel sistema delle fonti: uno studio comparato*, Cedam, Padova, 2008; E. BUCALO, *Autorità indipendenti e* soft law. *Forme, contenuti, limiti e tutele*, Giappichelli, Torino, 2018.

discussione, con una 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[62].

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[63], 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.

[62] Più approfonditamente sul punto, v. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., 287 ss.

[63] Cfr. A. SIMONCINI, *L'algoritmo incostituzionale*, cit., 89. A questo riguardo da qualche anno si è iniziato ad esplorare e costruire il filone del "costituzionalismo digitale", come tentativo di adattare i valori e gli istituti del costituzionalismo liberal-democratico al contesto tecnologico; cfr. C. PADOVANI, M. SANTANIELLO, *Digital constitutionalism: Fundamental rights and power limitation in the Internet eco-system*, in *The international communication gazette*, 80, 4, 2018, 295 ss.; E. CELESTE, *Digital constitutionalism: a new systematic theorisation*, in *International review of law, computers & technology*, 33, 1, 2019, 76 ss.; G. DE GREGORIO, *The rise of digital constitutionalism in the European Union*, in *International journal of constitutional law*, 19, 1, 2021, 41 ss.