Ritorno al futuro: le ragioni del costituzionalismo 1.0 nella regolamentazione della società algoritmica e della nuova economia a trazione tecnologica*

Riccardo de Caria

Abstract

La cosiddetta società algoritmica solleva indubbiamente molte sfide dal punto di vista del ruolo degli attori privati, e di quale sia il modo preferibile di regolamentarli da parte dello Stato. Tuttavia, questo tema ha già iniziato ad attirare una notevole attenzione da parte degli studiosi e dei policy-makers. In questo articolo, guardo alle sfide sollevate dalla società algoritmica dal punto di vista opposto, ovvero guardando allo Stato non come potenziale regolatore, ma come esso stesso soggetto al rispetto di alcune regole fondamentali. Troppo spesso, infatti, una domanda rimane inevasa: cosa succede, e quale dovrebbe essere il quadro giuridico, quando sono gli Stati ad accumulare massivamente informazioni e dati e ad usarli "contro" i loro cittadini?

Se combinata con il monopolio weberiano sull'uso legittimo della forza fisica, questa pratica crea una tremenda concentrazione di potere, che è estremamente pericolosa, perché sarebbe un'arma letale nelle mani di governi malintenzionati. Ma la situazione sembra meritevole di grande preoccupazione anche quando sono in gioco gli ordinamenti democratici.

Le minacce più immediate riguardano la libertà individuale nei seguenti campi, considerati singolarmente con esempi tratti da ricerche di carattere comparatistico: la censura di internet; la raccolta e l'uso di dati personali per fornire servizi pubblici; le indagini sulle frodi fiscali; altre indagini penali e prevenzione di minacce alla sicurezza pubblica.

L'articolo si conclude sostenendo la necessità di riscoprire, in questa epoca di profon-

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista.

Desidero ringraziare tutti i partecipanti al panel *Costituzionalismo e democrazia algoritmica* nel convegno di ICON-S Italian Chapter "Le nuove tecnologie e il futuro del diritto pubblico" svoltosi a Firenze il 22-23 novembre 2019 per i preziosi riscontri ricevuti in occasione della presentazione di una versione precedente del presente lavoro, nonché l'anonimo *reviewer* per le osservazioni molto utili e puntuali.

da trasformazione tecnologica, le ragioni originarie del costituzionalismo: la società algoritmica rende infatti quanto mai urgente riaffermare i vincoli costituzionali al potere governativo, al fine di impedire che i diritti fondamentali vengano annacquati, solo perché ciò è tecnologicamente possibile. Il costituzionalismo dovrebbe pertanto trovare nuovi strumenti per perseguire un vecchio obiettivo, anzi il più antico, cioè limitare i poteri del governo. In definitiva, per affrontare le molte sfide della società algoritmica, potrebbe occorrere qualche forma di costituzionalismo 4.0, ma sicuramente vi è ancora bisogno anche del "buon vecchio" costituzionalismo 1.0.

The so-called algorithmic society undoubtedly raises many challenges from the point of view of the role of private actors, and what is the preferred way of regulating them by the government. However, this issue has already begun to attract considerable attention from scholars and policy-makers. In this article, I consider the challenges raised by the algorithmic society from the opposite point of view, i.e. by looking at the government not as a potential regulator, but as itself subject to some fundamental rules. All too often, in fact, one question remains unanswered: what happens, and what should the legal framework be, when it is the governments that massively accumulate information and data and use them "against" their citizens?

When combined with the Weberian monopoly on the legitimate use of physical force, this practice creates a tremendous concentration of power, which is extremely dangerous, because it would be a lethal weapon in the hands of malicious governments. But the situation seems worthy of great concern even when democratic systems are at stake.

The most immediate threats concern individual freedom in the following fields, considered individually with examples taken from comparative research: internet censorship; the collection and use of personal data to provide public services; tax fraud investigations; other criminal investigations and prevention of threats to public security.

The article concludes by arguing the need to rediscover, in this era of profound technological transformation, the original reasons for constitutionalism: the algorithmic society makes it all the more urgent to reaffirm the constitutional constraints to government power, in order to prevent fundamental rights from being watered down, just because this is technologically possible. Constitutionalism should therefore find new instruments to pursue an old objective, to be sure the oldest one, namely to limit the powers of government. Ultimately, some form of constitutionalism 4.0 may be needed to meet the many challenges of the algorithmic society, but surely there is still a need for "good old" constitutionalism 1.0 as well.

Keywords

società algoritmica - stato di sorveglianza - diritti fondamentali - big data - nuove tecnologie

1. Introduzione: tra *surveillance capitalism* e *surveillance state*

La cosiddetta società algoritmica solleva indubbiamente molte questioni dal punto di vista del ruolo dei grandi attori privati, a cominciare dalle piattaforme, e di quale sia la via preferibile per gli Stati nel regolamentarli[1]. Si è parlato a proposito di capitalismo di sorveglianza[2]; in quest'ottica, un recente report di Amnesty International ha ad esempio affermato che il modello di business di attori come Google e Facebook costituirebbe una minaccia per i diritti umani[3]; addirittura, alcuni autorevoli autori hanno sostenuto che, con riferimento agli over the top o ai cosiddetti GAFA (noto acronimo per Google, Apple, Facebook, Amazon), si debba ribaltare la "*presumption of liberty*"[4] e applicare invece la regola aurea relativa alla pubblica amministrazione per cui a tali colossi privati dovrebbe applicarsi l'opposto principio per cui ad essi è permesso fare solo ciò a cui sono espressamente autorizzati da una norma di legge, stanti appunto le loro dimensioni e il loro ruolo, che ne farebbero appunto un soggetto equiparabile a quelli di natura pubblica[5].

Personalmente sono in forte disaccordo con tale impostazione: basti dire che qualunque over the top appare assoggettato a regole pubblicistiche vincolanti e spesso invasive come quelle in materia di concorrenza, per cui – a dispetto dei fuorvianti confronti tra fatturato e PIL, o tra numero di utenti e numero di cittadini, che talvolta vengono proposti in sede giornalistica[6] – qualunque stato sovrano per quanto piccolo ha, in virtù del monopolio legale sull'uso della forza, più potere di qualunque over the top, a prescindere dalla quantità e qualità di dati personali di cui esso disponga.

In questa sede, però, vorrei soltanto prendere questa impostazione come esempio di un dibattito che, pur appunto orientato in prevalenza in una direzione non necessariamente condivisibile, certamente esiste ed è ampiamente coltivato, a diversi livelli e in diverse giurisdizioni, con il coinvolgimento di *scholars*, *policy-makers*, operatori, esperti e opinione pubblica.

Ciò di cui invece intendo occuparmi in questa sede è invece il fenomeno opposto, ov-

---

[1] Cfr. in argomento, tra i molti, G. De Gregorio, *From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society*, in *European Journal of Legal Studies,* 11(2), 2019, 65 ss.; M. Monti, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale,* in *Rivista italiana di informatica e diritto,* 1, 2019, 35 ss.; Id., *Perspectives on the regulation of search engine algorithms and social networks: The necessity of protecting the freedom of information*, in *Opinio Juris,* 1, 2017, 71 ss.

[2] V. ad esempio S. Zuboff, *The Age of Surveillance Capitalism*, London, 2019.

[3] Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*, Amnesty International, London, 2019. V. anche la poderosa inchiesta di S.A. Thompson e C. Warzel per il Privacy Project del New York Times, *Twelve Million Phones, One Dataset, Zero Privacy*, New York Times, 19 dicembre 2019.

[4] Così un pregevole lavoro di R. Barnett, *Restoring the Lost Constitution: The Presumption of Liberty*, Princeton-Oxford, 2014 (2004).

[5] Così ad es. G. De Minico al convegno internazionale *Insert Law to Continue*, tenutosi a Napoli il 12-13 settembre 2019. Di questa Autrice, si veda tra gli altri *Libertà digitali. Luci e ombre*, Torino, 2018.

[6] Cfr. perfino il World Economic Forum, rispettivamente J. Myers, *How do the world's biggest companies compare to the biggest economies?*, 19 otttobre 2016; e H. Taylor, *If social networks were countries, which would they be?*, 28 aprile 2016.

vero il *surveillance state*[7], e ciò perché esso ha a mio avviso ricevuto sin qui un'attenzione sorprendentemente limitata, in relazione ai rischi che può comportare per la tutela dei tradizionali diritti di libertà, secondo me di gran lunga superiori a quelli portati dal cosiddetto *surveillance capitalism*.

Intendo dunque occuparmi di come le nuove tecnologie offrano ai governi il potere di mettere in atto la prospettiva distopica di un panopticon[8] digitale, che alla disponibilità di una enorme quantità di informazioni e dati personali – il cosiddetto oro o petrolio del terzo millennio[9] – unisce appunto il monopolio legale sull'uso della forza, generando una concentrazione di potere potenzialmente pericolosissima, e ciò già nelle democrazie, a maggior ragione nei non pochi regimi autoritari del mondo (rimane a proposito imperitura la nota massima di Lord Acton per cui «*Power tends to corrupt; absolute power corrupts absolutely*»[10]).

Nelle pagine che seguono, guarderò quindi alle sfide della società algoritmica considerando gli Stati non come potenziali regolatori, ma come essi stessi assoggettati (o da assoggettare) a regole fondamentali: in che misura, mi chiederò dunque, gli Stati sono (o dovrebbero) essere tenuti a rispettare le regole da essi stessi imposte agli attori privati? Come accennato appena sopra, non si tratta di un tema che riguardi solo ordinamenti dove si sia lontani dal raggiungimento dei più alti standard democratici, ma anche delle consolidate democrazie occidentali[11], che purtroppo offrono molti esempi discutibili e pericolosi (ma legittimi?) di impiego della gran messe di informazioni e dati che la tecnologia mette a loro disposizione.

Seguirò un percorso insieme per temi e per Paese, soffermandomi su una serie di ambiti a mio avviso particolarmente significativi, che – nell'impossibilità, in questa sede, di trattare singolarmente in modo diffuso – illustrerò per il tramite di alcuni esempi provenienti da reali vicende legislative, di policy o giudiziarie di alcuni ordinamenti rilevanti, in prevalenza recenti o molto recenti. Tratterò dapprima il tema della censura di internet ad opera dei governi (§ 2), per poi soffermarmi su alcuni casi di raccolta e utilizzo di dati personali per finalità collegate all'erogazione di servizi pubblici (§ 3), quindi tratterò il tema delle indagini fiscali (§ 4), e infine affronterò la questione della pervasività dei poteri di indagine delle autorità inquirenti in materia penale (§ 5.). Nella conclusione presenterò alcune osservazioni finali a sostegno della mia tesi (§ 6).

Qualche considerazione metodologica s'impone ancora con riferimento alla selezione di tali ambiti, degli ordinamenti considerati, e conseguentemente dei casi trattati, come

---

[7] Possiamo definirlo come «*a state that aims at preventive, everyday, mass surveillance*»: così P. Lemieux, *Why the Surveillance State is Dangerous, The Library of Economics and Liberty*, 10 June 2018; in argomento, v. anche, tra i molti, J.M. Balkin, *The Constitution in the National Surveillance State*, in *Minn. L. Rev.,* 93, 2008, 1 ss. Per alcune interessanti riflessioni, v. anche M.C. Cavallaro-G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it,* 16, 19, 4 settembre 2019, spec. 7 ss..

[8] Il riferimento è naturalmente alle lettere al padre del filosofo inglese J. Bentham, raccolte nel noto *Panopticon or the Inspection-House*.

[9] Cfr. The Economist, *The world's most valuable resource is no longer oil, but data*, 6 maggio 2017.

[10] Formulata in una lettera al vescovo Mandell Creighton nel 1987.

[11] Le cosiddette "democrazie stabilizzate": cfr. T.E. Frosini (a cura di), *Diritto pubblico comparato. Le democrazie stabilizzate*, Bologna, 2019.

noto tema sempre piuttosto delicato e controverso[12].

Gli argomenti testé indicati appaiono rappresentare le principali declinazioni del rapporto problematico tra nuove tecnologie e potere statale, tema di questo lavoro. Essi corrispondono abbastanza distintamente ad alcuni diritti fondamentali, che vengono di volta in volta in rilievo, e che sono dunque i riferimenti costituzionali che l'analisi dovrà sempre tener presenti sullo sfondo: per la censura, la libertà di manifestazione del pensiero e di stampa; per la raccolta di informazioni biometriche, il diritto alla riservatezza; per la materia fiscale, il diritto di proprietà; per l'ambito penale, la libertà personale.

Appaiono infatti questi i diritti più direttamente esposti ad una possibile compressione per effetto delle opportunità offerte ai governi dalle nuove tecnologie, e appaiono esserlo più di altri, dove invece si pongono, o quanto meno si sono poste sin qui, questioni assai meno problematiche: si pensi, solo per fare alcuni esempi, ad altre libertà civili come la libertà di associazione e riunione o la libertà religiosa, o alla libertà di iniziativa economica, o ancora ai diritti sociali. Si tratta evidentemente di ambiti di grandissima importanza, dove però le nuove tecnologie non sembrano dare ai governi quel potere di interferenza che si manifesta invece nei settori considerati.

Va da sé che ciascun ordinamento ha poi le sue peculiarità, nella ricostruzione prima ancora che nella protezione dei vari diritti fondamentali che vengono in rilievo, ma che i diritti fondamentali maggiormente rilevanti siano quelli individuati appare valido a prescindere dal contesto e dalla latitudine: a prescindere dalle idiosincrasie anche terminologiche locali, ad essere coinvolte un po' ovunque sono tendenzialmente quelle che nel nostro linguaggio costituzionale chiamiamo libertà di opinione, diritto alla riservatezza, proprietà e libertà personale. I primi due sono strettamente connessi e dunque vanno trattati di seguito l'uno all'altro; a loro volta, proprietà e libertà personale appaiono accomunati dall'essere ambiti non certamente nuovi (così come invece pongono problemi nuovi internet e ad es. le tecniche di riconoscimento facciale), ma dove le nuove tecnologie permettono agli Stati di compiere un salto di qualità notevolissimo nel perseguimento di scopi che, di per sé, hanno sempre avuto.

Fermo restando questo, la comparazione sarà qui inevitabilmente asimmetrica: le vicende giudiziarie si sviluppano con una inevitabile dose di casualità nei vari ordinamenti, non presentandosi necessariamente un medesimo caso in tutti gli ordinamenti che si vogliono considerare. Pertanto, nell'impossibilità di trovare sempre un termine confronto specifico, si accetterà qui una certa dose di *serendipity* nel selezionare importanti casi problematici, italiani e di ordinamenti stranieri, con particolare interesse per quelli appartenenti alla "famiglia a egemonia professionale", secondo la classificazione di Mattei[13].

Se, infatti, come già detto, l'impiego delle nuove tecnologie in ordinamenti "a egemonia politica" sorprende meno, pur mantenendo certamente interesse nel costituire un indubbio strumento di rallentamento della transizione che li riguarda, è nelle de-

[12] Cfr. al riguardo i profondi insegnamenti di R. Hirschl, *The Question of Case Selection in Comparative Constitutional Law*, in *Am J. Comp. L.,* 53(1), 2005, 125 ss.

[13] U. Mattei, *Three Patterns of Law: Taxonomy and Change in the World's Legal Systems*, in *Am. J. Comp. L.,* 45(1), 1997, 5 ss.

mocrazie compiute che tale fenomeno appare più meritevole di riflessione, in quanto fonte di potenziali inedite involuzioni e ritorni al passato, difficili da immaginare da prospettiva storicistica, ma pur sempre possibili.
I casi verranno considerati dunque là dove essi si sono presentati, seguendo così prima di tutto le cronache politico-giudiziarie, inevitabile punto di riferimento prima che si consolidi la letteratura scientifica. Senz'altro qualcosa mancherà e qualcosa sarà sfuggito, ma la convinzione e l'auspicio è che i casi che si esporranno delineino un quadro sufficientemente preciso della natura e dei rischi del "*surveillance state*", e della difficoltà che si riscontra nel reagire a tale evoluzione con gli strumenti del rimedio giurisdizionale.

2. Censura di internet

Il primo tema considerato, la censura del web, è uno di quelli evidentemente più vasti: come noto, in molti ordinamenti, tra cui la Cina, esiste un controllo governativo sull'accesso ad internet da parte dei cittadini, un enorme firewall che filtra i contenuti ed è in grado di monitorare il comportamento online degli utenti con estrema pervasività[14].
Ciò che appare particolarmente interessante è, a questo proposito, il tema dei rimedi. Da questo punto di vista, vorrei menzionare la sentenza della Corte costituzionale turca del luglio 2019. In Turchia, a seguito fallito colpo di stato del luglio 2016, il governo ha reso particolarmente stringenti i già esistenti controlli su siti internet[15] e social media[16] (oltre a procedere a molti arresti per reati d'opinione di persone critiche verso il governo stesso).
Alcuni accademici hanno sottoposto alla Corte la questione della legittimità del blocco di alcuni account Twitter e domini riconducibili a oppositori del governo, tuttavia la Corte costituzionale ha recentemente rigettato le loro domande, escludendo il loro interesse ad agire in quanto non vittime dirette della censura[17]. La vicenda appare di-

[14] In particolare sulla Cina, v. X. Xu-Z.M. Mao-J.A. Halderman, *Internet Censorship in China: Where Does the Filtering Occur?*, in N. Spring-G.F. Riley (eds.), *Passive and Active Measurement. PAM 2011. Lecture Notes in Computer Science*, vol. 6579, Berlin-Heidelberg, 2011.

[15] Quasi 250.000 siti web e domini tra 2014 e 2018, secondo un report della Istanbul Freedom of Expression Association (İFÖD): cfr. la notizia su AhvalNews, *Turkey bans access to almost 300,000 websites since 2006 - reports*; cfr. anche il resoconto aggiornato di D. Jones, *Turkey's New Internet Regulations Spark Fears of New Wave of Censorship*, VOANews, 8 ottobre 2019.

[16] Una limitazione divenuta poi blocco tout-court in circostanze specifiche: cfr. P. Martineau, *Turkish ISP Blocks Social Media Sites Near Syrian Border*, Wired, 18 novembre 2019, dove si riferisce che «*Partially government-owned Türk Telekom restricted access to Facebook, Instagram, Twitter, and WhatsApp for about 48 hours as Turkey attacked the Kurds*». La pratica di bloccare l'accesso al web in risposta a supposte emergenze di ordine pubblico, comunque, è stata adottata anche in ordinamenti democratici come quello indiano: cfr. A. Muglia, *L'India per la prima volta spegne web e cellulari anche a Delhi. Ma i cortei si estendono in tutto il Paese*, in *Corriere.it*, 19 dicembre 2019.

[17] Corte costituzionale turca, sentenze *Kerem Altıparmak and Yaman Akdeniz (2),* 2015/15977, 12 giugno 2019 e *Kerem Altıparmak and Yaman Akdeniz (4)*, 2015/18876, 19 Novembre 2019. Tali iniziative giudiziarie sono state solo le ultime in ordine di tempo intraprese dal Prof. Akdeniz, individualmente o col collega Altiparmak e altri soggetti; in passato, Akdeniz e i suoi colleghi di *strategic litigation* avevano

mostrare come le corti non sempre siano validi baluardi contro tentativi degli organi politici di restringere una libertà fondamentale come quella di stampa e manifestazione del pensiero, di cui la libertà di internet è espressione.

Questo caso, al di là della dimostrazione di un effettivo e persistente controllo su internet dei governi anche di Paesi membri di istituzioni come il Consiglio d'Europa, resistente anche appunto al controllo giurisdizionale, si connette anche ad un altro tema, quello dell'over-enforcement della normativa contro l'hate-speech e dei rischi che questo comporta.

In effetti, ciò che accade con la normativa sull'*hate speech* è che, in assenza di un online *due process*[18], si rischia di ridurre al silenzio delle forme di espressione dei cittadini che meriterebbero invece di poter essere manifestate. Ciò accade appunto con la normativa sull'hate speech ma il discorso si può estendere a tutti i tentativi normativi di disciplinare il fenomeno delle cosiddette fake news[19]. Ebbene, io credo che si possa tracciare un parallelismo con il caso turco appena ricordato, dal momento che molto spesso i governi hanno buon gioco nel giustificare la censura sulla base di normative dallo scopo apparentemente condivisibile, quali il contrasto al terrorismo o minacce all'ordine pubblico in generale (o appunto l'*hate speech*).

Così, sempre nel caso turco, sono paradossalmente i media sostenitori della causa curda a patire forme di censura, sulla base di norme che apparentemente dovrebbero offrire strumenti di lotta alla propaganda terrorista, ma che in mano al governo vengono pervertite per silenziare invece le minoranze[20].

Del resto, il quadro non è così monolitico, come dimostra una recentissima sentenza della stessa Corte costituzionale turca, che ha invece dichiarato contrario alla libertà di espressione il blocco dell'accesso a tutta Wikipedia, che era stato introdotto per reazione al contenuto di due specifiche voci ("*Foreign Involvement in the Syrian Civil War*" and "*State-sponsored Terrorism*"), nell'impossibilità di bloccare solo quelle e dovendo, per bloccare quelle, inibire l'accesso a tutto il sito[21]. La sentenza, che peraltro ha ricevuto

avuto ad es. successo nell'ottenere invece dalla Corte costituzionale turca un ordine alle autorità del Paese di sbloccare l'accesso a Twitter: così nel caso *Yaman Akdeniz et al.*, B. No: 2014/3986, 2 Aprile 2014. Altri casi invece lo avevano visto soccombere davanti alla giurisdizione nazionale, con la conseguente scelta di rivolgersi allora alla Corte europea dei diritti dell'uomo, talvolta con successo (*Cengiz and Others c. Turchia*, ricc. 48226/10 e 14027/11 (2015)), talatra no (*Akdeniz c. Turchia,* ric. 20877/10, decisione dell'11 marzo 2014 di inammissibilità): v. un quadro riepilogativo aggiornato a fine 2018 ad opera di S. Crozier, *Turkish Lawyer Battles through the Courts to Protect Freedom of Expression*, sul sito di *European Endowment for Democracy*, 8 novembre 2018. Del Prof. Akdeniz, merita citare tra gli altri anche il suo scritto *To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression*, in M.V. De Azevedo Cunha et al. (eds.), *New Technologies and Human Rights: Challenges to Regulation*, London-New York, 2013, 47 ss.

[18] M. Husovec, *Why There Is No Due Process Online?*, in *Balkinization*, 7 giugno 2019.

[19] In argomento, tra i moltissimi si veda, su questa Rivista, M. Bassini-G.E. Vigevani, *Primi appunti su fake news e dintorni*, in *questa Rivista*, 1, 2017, 11 ss.

[20] Cfr. già il caso *Sürek and Özdemir v. Turkey* deciso dalla Corte EDU l'8 luglio 1999, ricc. 23927/94 e 24277/94; v. anche in argomento M.C. Ünal, *Counterterrorism in Turkey: Policy Choices and Policy Effects toward the Kurdistan Workers' Party (PKK)*, Abingdon-New York, 2013.

[21] Sentenza *Wikimedia Foundation Inc. et al.* [GK], B. No: 2017/22355, 26 dicembre 2019. Il caso era stato nel frattempo portato anche davanti alla Corte europea dei diritti dell'uomo, *Wikimedia Foundation, INC. c. Turchia*, ric. 25479/19.

applicazione solo dopo alcune settimane[22], dimostra che esistono spazi per un'effettività del rimedio giurisdizionale nei confronti delle restrizioni alla libertà di espressione su internet anche in ordinamenti come quello turco, ma la mancata attuazione immediata è parimenti dimostrazione di come talvolta neppure un esito favorevole di un'iniziativa giurisdizionale sia sufficiente.

Il tema dell'accesso a internet è stato oggetto di riflessione, da un punto di vista diverso ma che è interessante confrontare con quanto visto sin qui, anche in altri ordinamenti. Vorrei in particolare ricordare una sentenza della Corte Suprema degli Stati Uniti nel 2017, che ha ritenuto contrario al Primo Emendamento alla Costituzione americana, che tutela come noto la libertà di espressione, il divieto di accesso ai social media che la legislazione della North Carolina aveva previsto come sanzione accessoria per i condannati per reati sessuali[23].

Il giudice Kennedy, scrivendo per una corte unanime nel giudizio, ha in effetti riconosciuto il ruolo fondamentale che hanno internet e i social media nel garantire la piena effettività del diritto ad informare ed essere informati, che secondo la Corte non deve essere compresso neppure nel caso di autori di reati particolarmente odiosi: «*access to what for many are the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge. These websites can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard. They allow a person with an Internet connection to "become a town crier with a voice that resonates farther than it could from any soapbox*." *Reno*, 521 U.S., *at* 870. *In sum, to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights. It is unsettling to suggest that only a limited set of websites can be used even by persons who have completed their sentences. Even convicted criminals—and in some instances especially convicted criminals—might receive legitimate benefits from these means for access to the world of ideas, in particular if they seek to reform and to pursue lawful and rewarding lives*».

La sentenza americana può a sua volta essere utilmente confrontata con una italiana, che ha riguardato il caso della chiusura, da parte di Facebook, di alcune pagine e profili riconducibili ad un movimento italiano di estrema destra, Casa Pound. Casa Pound ha impugnato tale decisione con procedura d'urgenza davanti al giudice civile, e nel momento in cui scrivo il Tribunale di Roma ha emesso un'ordinanza cautelare in cui ha ordinato a Facebook di riattivare le pagine e i profili in questione, sulla base di considerazioni non dissimili da quelle della Corte Suprema americana a proposito del ruolo imprescindibile assunto da Facebook come strumento di partecipazione al dibattito pubblico, cui hanno diritto di partecipare anche movimenti estremisti – ma non fuorilegge – come Casa Pound: «il rilievo preminente assunto dal servizio di Facebook (o di altri social network ad esso collegati) con riferimento all'attuazione di principi cardine essenziali dell'ordinamento come quello del pluralismo dei partiti politici (49 Cost.), al punto che il soggetto che non è presente su Facebook è di fatto escluso (o fortemente limitato) dal dibattito politico italiano, come testimoniato dal fatto che la quasi totalità

[22] In particolare, dal 15 gennaio 2020: cfr. la notizia su HürrietDailyNews, *Wikipedia ban lifted after top court ruling issued*, 15 gennaio 2020.

[23] *Packingham v. North Carolina*, 582 U.S. ___ (2017).

degli esponenti politici italiani quotidianamente affida alla propria pagina Facebook i messaggi politici e la diffusione delle idee del proprio movimento. Ne deriva che il rapporto tra Facebook e l'utente che intenda registrarsi al servizio (o con l'utente già abilitato al servizio come nel caso in esame) non è assimilabile al rapporto tra due soggetti privati qualsiasi in quanto una delle parti, appunto Facebook, ricopre una speciale posizione: tale speciale posizione comporta che Facebook, nella contrattazione con gli utenti, debba strettamente attenersi al rispetto dei principi costituzionali e ordinamentali finché non si dimostri (con accertamento da compiere attraverso una fase a cognizione piena) la loro violazione da parte dell'utente»[24].

A ben vedere, vi è in realtà una fondamentale differenza tra il caso americano e quello italiano: nel primo caso le restrizioni all'accesso ad internet erano dettate da una legge, dunque per iniziativa del potere pubblico, mentre nel secondo si trattava di un rapporto esclusivamente tra soggetti privati. Il giudice italiano ha aderito all'opinione che citavo all'inizio, e che come ricordavo gode di molti consensi nella letteratura giuridica, per cui Facebook va trattato come un soggetto pubblico; se tale premessa appare di per sé molto discutibile, appare però condivisibile la conseguenza che ne trae il giudice italiano una volta che la ha fatta propria, ovvero che non è possibile restringere l'accesso ad internet, se non eventualmente in casi estremamente gravi e circoscritti.

Il quadro che ne deriva in materia di *Internet censorship* appare dunque in chiaroscuro a livello mondiale: esistono infatti segnali inequivocabili del tentativo dei pubblici poteri di restringere o comunque controllare l'accesso al mercato delle idee online, spesso facendosi scudo di una legislazione apparentemente dettata con finalità di protezione della democrazia. In alcuni casi, simili tentativi incontrano un freno nelle corti, in altri invece il rimedio giurisdizionale appare ineffettivo.

3. Uso dei dati per determinare premialità o punizioni o comunque accedere ai servizi

Un diverso ordine di casi di possibile realizzazione del *surveillance state* è accomunato dalla finalità con cui vengono raccolti i dati personali dei cittadini, ovvero l'erogazione di servizi o comunque trattamenti individualizzati sulla base delle caratteristiche personali di ciascuno di essi.

L'esempio più eclatante è quello del cosiddetto "*social credit system*" cinese, gigantesco programma di ingegneria sociale su cui esiste una letteratura per la verità abbastanza contraddittoria: alcuni studi infatti lo descrivono come il più grande esperimento di realizzazione del Grande Fratello di Orwell mai realizzato[25], mentre altri ne danno una lettura meno preoccupata[26].

Certamente, anche nella versione più soft, esso appare una forma di invasione della

[24] Trib. Roma, sez. spec. impresa, ordinanza 12 dicembre 2019.

[25] L. Orgad-W. Reijers, *A Dystopian Future? The Rise of Social Credit Systems*, Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS 2019/94.

[26] D. Mac Síthigh-M. Siems, *The Chinese social credit system: A model for other countries?*, EUI Working Paper LAW 2019/01.

riservatezza davvero notevole, tanto più che i dati necessari ad assegnare ai cittadini i punteggi per le loro azioni e poi premiarli o punirli di conseguenza verrebbero raccolti, a quanto pare, non in forma aggregata e anonima, ma con specifico riferimento ai comportamenti di ciascuno.
Tramite l'incrocio di una serie di strumenti tecnologici, verrebbero così tracciati gli spostamenti e le azioni, offline e online, potenzialmente di tutti i cittadini e delle imprese, così da avere un quadro aggiornato in tempo reale del modo in cui si comportano, con una compressione della riservatezza che non ha eguali in nessun altro ordinamento.
Va detto peraltro che il sistema cinese, per quanto estremo nella sua concezione, appare comunque avere alcune affinità con altri meccanismi, pur diversi, in via di introduzione in altri ordinamenti. Mi riferisco a quei Paesi che hanno realizzato o stanno realizzando forme di riconoscimento facciale (o altre forme di riconoscimento biometrico) per costruire delle identità digitali che daranno accesso ai servizi pubblici[27]. È il caso, anche qui, della Cina[28], ma anche di Singapore, dell'India, e della Francia[29], che ha di recente introdotto il suo sistema ALICEM, che ha sollevato accese discussioni ed è anche oggetto di un tentativo di fermarlo per via giudiziaria da parte dell'authority francese sulla privacy, per via delle forti interferenze con la tutela della riservatezza che un sistema di questo tipo comporta[30]. Anche in Italia vi sono state molto di recente polemiche con riferimento alla proposta del ministro dell'innovazione di introdurre una forma di identità digitale gestita dallo Stato, per timori legati anche in questo caso alla tutela della riservatezza[31].
In definitiva, anche sotto questo aspetto appare concreto il rischio di invasione della sfera personale dei cittadini da parte delle pubbliche autorità, anche in questo caso con finalità almeno in parte formalmente ineccepibili, ma che nei fatti possono condurre ad una pericolosissima compressione delle libertà personali.

4. Ambito fiscale

Veniamo ora a trattare, se pur molto brevemente per le esigenze di questa trattazione,

[27] Il riconoscimento facciale è al centro delle attività anche di società private, che poi possono decidere di collaborare con le autorità, mettendo a loro disposizione la loro capacità di associare un'immagine di una persona a foto di quella stessa persona presenti online, tramite il loro enorme database: è il caso di Clearview AI, su cui cfr. K. Hill, *The Secretive Company That Might End Privacy as We Know It*, in *The New York Times*, 18 gennaio 2020.

[28] In accoppiamento con una raccolta massiva di DNA umano: così Z. Evans, *China Collects Human DNA En Masse to Advance Facial Recognition Techniques*, in *National Review*, 3 dicembre 2019.

[29] Cfr. H. Fouquet, *France Set to Roll Out Nationwide Facial Recognition ID Program,* in. *Bloomberg*, 3 ottobre 2019. Recenti fonti giornalistiche (J. Delcker-B. Smith-Meyer, *EU considers temporary ban on facial recognition in public spaces*, in *Politico.com*, 17 gennaio 2020) hanno invece riferito di una proposta su cui è al lavoro la Commissione Europea per introdurre un divieto di cinque anni a forme di riconoscimento facciale in pubblico.

[30] Mentre il presente lavoro viene redatto, il caso non è ancora stato deciso.

[31] Cfr. News1, *Digital identity, Minister Pisano: "The state should give citizens unique user names and passwords". It's controversy*, 4 gennaio 2020.

della materia fiscale, che appare senza dubbio uno degli ambiti in cui appaiono più dirompenti le conseguenze della disponibilità, da parte dei pubblici poteri, di potenti strumenti tecnologici di indagine e raccolta dati. Da questo punto di vista, il caso italiano è forse uno dei più significativi.

Secondo una recente indagine relativa appunto all'Italia, «il Fisco fa il pieno di banche dati. Sono ben 31, e non sono nemmeno tutte: il numero, infatti, fa riferimento solo ai principali centri di raccolta fiscali. A fornire il dato di questa overdose informativa è Massimo Bitonci, sottosegretario del ministero dell'economia, nel corso dell'audizione alla Commissione di vigilanza sull'anagrafe tributaria, presieduta da Ugo Parolo (Lega), tenutasi ieri. Un sistema informativo notevole, dunque, che serve tutta l'area della fiscalità, ovvero il Dipartimento delle finanze del Mef (Ministero dell'economia e finanza), le Agenzie fiscali, l'Agenzia delle entrate-Riscossione e la Guardia di finanza. Inoltre, se si tiene conto, delle banche dati della pubblica amministrazione il numero sale a 129, secondo i dati, datati 2013, dell'ultima indagine resa disponibile dalla stessa Commissione»[32].

In questo caso, i dati vengono raccolti in forma aggregata e anonima, ma nel momento in cui il sistema informatico segnala agli operatori del fisco anomalie risultanti dall'incrocio di dati presenti in qualcuna delle numerose banche dati ora ricordate, non vi sono ostacoli all'immediata identificazione del sospettato.

Tale tendenza[33], nonostante le critiche dell'autorità garante della privacy[34], è stata di recente ancor più approfondita con l'approvazione del cosiddetto decreto fiscale, 26 ottobre 2019, n. 124, convertito con modificazioni dalla legge 19 dicembre 2019, n. 157: tutto il capo primo contiene "Misure di contrasto all'evasione fiscale e contributiva ed alle frodi fiscali", e tra le altre cose prevede un allargamento delle possibilità di utilizzo delle banche dati contenenti le fatture elettroniche per le indagini di polizia economico-finanziaria[35].

Ma queste disposizioni non fanno altro che confermare una chiara direzione già intrapresa dalle autorità italiane (se pur ancora senza fare un ulteriore passo in avanti compiuto invece in tempi recentissimi dal legislatore francese, come dirò tra un momento). Un ottimo scritto di carattere giornalistico[36] ricordava in particolare la circolare n. 16/E del 28 aprile 2016 dell'Agenzia delle Entrate, che, nel delineare gli indirizzi operativi per la prevenzione e il contrasto all'evasione fiscale, chiariva che «al punto di vista operativo, alle notizie ritraibili dalle banche dati si aggiungono quelle che perven-

---

[32] V. Morena, *Il fisco fa il pieno di banche dati*, in *ItaliaOggi*, 7 marzo 2019; cfr. anche M. Damiani, *Banche dati del Fisco: un eccesso informativo da razionalizzare. Quali scenari?*, in *Ipsoa.it*, 30 marzo 2019.

[33] Che peraltro si inserisce nel quadro di una ben nota tendenza internazionale allo scambio transfrontaliero di informazioni bancarie raccolte a livello interno: sui profili problematici che questo comporta a livello europeo, cfr. ad esempio M.G.H. Schaper, *Data Protection Rights and Tax Information Exchange in the European Union: An Uneasy Combination*, in *Maastricht Journal of European and Comparative Law,* 23(3), 2016, 514 ss.

[34] A. Cherchi, *La lotta all'evasione con i super-archivi nel mirino del Garante della privacy*, in *il Sole 24 Ore*, 15 novembre 2019.

[35] R. Imparato, *Fattura elettronica, controlli a tappeto dal 2020: tutti i dati al Fisco per 8 anni*, in *Money.it*, 18 dicembre 2019.

[36] A. Scaglioni, *Evasione, da social network e big data la nuova caccia ai «furbetti»*, in *Corriere.it*, 12 gennaio 2020.

gono da altre fonti, ivi incluse fonti aperte»[37]; nonché, similmente, la circolare 1/2018 della Guardia di Finanza, del 4 dicembre 2017, che impegnava il Corpo alla «eventuale ricerca di altri elementi utili non risultanti dalle citate banche dati, anche presso gli Uffici e gli Enti pubblici presenti sul territorio, previa adozione delle necessarie cautele per garantire l'indispensabile riservatezza dell'attività da intraprendere. In tale contesto, deve essere posta particolare attenzione alla consultazione delle c.d. "fonti aperte" (articoli stampa, siti internet, social network, ecc.) al fine di acquisire ogni utile elemento di conoscenza sul contribuente da sottoporre a controllo e sull'attività da questi esercitata»[38]. In tempi recentissimi, tale orientamento ha ricevuto un importante avallo dalla Corte di Cassazione, con la sentenza n. 308/2020, che ha ritenuto legittimo un accertamento fiscale fondato su immagini prelevate da Google Street View.

Da ultimo, appare significativo un recentissimo dato di carattere comparatistico, ovvero la decisione n. 2019-796 del Consiglio costituzionale francese[39], che ha dichiarato compatibile con la costituzione l'articolo 154 della *loi de finances pour 2020*, che «autorise, à titre expérimental et pour une durée de trois ans, les administrations fiscale et douanière à collecter et à exploiter de manière automatisée les contenus accessibles publiquement sur les sites internet de certains opérateurs de plateforme, aux fins de recherche de manquements et d'infractions en matière fiscale et douanière» (§ 75). Per quel che qui viene in rilievo, i ricorrenti imputavano a tale disposizione il fatto di «*instaurer un dispositif de surveillance sur internet qui porterait une atteinte inconstitutionnelle au droit au respect de la vie privée, au droit à la protection des données personnelles et, dès lors qu'il conduirait les utilisateurs d'internet à s'autocensurer, à la liberté d'expression et de communication*» (§ 76); peraltro, a differenza che in Italia, il sistema prevede che la raccolta di big data può fungere da notizia di reato o comunque di infrazione fiscale, e dunque questi dati non vengono impiegati solo a conferma di indagini già aperte[40].

Tuttavia, l'organo di giustizia costituzionale francese ha ritenuto che fosse nel complesso accettabile il bilanciamento operato dal legislatore «*entre l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscales et le droit au respect de la vie privée*» (§ 80): la limitazione a quest'ultima e alla libertà di espressione è in effetti presente, ma – purché vengano rispettati alcuni limiti che vengono specificati in via di interpretazione, tra cui la libera disponibilità delle informazioni, che devono essere reperibili senza necessità di password d'accesso – la disposizione (salvo un breve inciso) risulta compatibile con la costituzione, anche quando prevede una raccolta dati in forma anonima e aggregata che poi funga da base per avviare un'investigazione (purché poi un'individualizzazione dei dati venga effettuata).

Appare dunque evidente una tendenza del legislatore, tanto italiano quanto francese negli esempi fatti, ad avvalersi delle possibilità offerte dalle nuove tecnologie per superare le garanzie di libertà personale in ambito fiscale. Tale tendenza trova un freno

[37] Agenzia delle Entrate, *Circolare n. 16/E, Anno 2016 - Prevenzione e contrasto all'evasione – Indirizzi operativi*, 28 aprile 2016, spec. 9.

[38] Comando Generale della Guardia di Finanzia, III Reparto Operazioni – Ufficio Tutela Entrate, *Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali*, vol. II, parte III, spec. 5.

[39] Décision n° 2019-796 DC du 27 décembre 2019.

[40] V. ancora A. Scaglioni, *op. cit.*

soltanto parziale o indiretto nella giurisprudenza, sia ordinaria sia costituzionale (da quest'ultimo punto di vista, oltre a quanto ricordato a proposito dell'ordinamento francese, si pensi all'affermazione di segno contrario fatta dalla Corte costituzionale italiana con il rinvio pregiudiziale alla CGUE – e in definitiva da quest'ultima accettata, se pur *obtorto collo* – nel notissimo caso *Taricco*[41]). Ancora una volta dunque la fotografia che si ricava è mista, con spinte verso la realizzazione anche in questo ambito del surveillance state, e solo limitate resistenze a livello giurisdizionale.

5. Indagini penali e sicurezza pubblica in genere

Un campo contiguo ma diverso è infine quello dell'impiego delle nuove tecnologie in indagini di carattere penale o comunque per perseguire, in via preventiva rispetto alla possibile commissione di reati, finalità di sicurezza pubblica.

Da questo punto di vista, l'ordinamento italiano si contraddistingue per un uso sempre più pervasivo, e ancora ampliato di recente dalla cosiddetta legge spazzacorrotti[42], dei captatori informatici per indagini penali (i cosiddetti trojan di stato), con riferimento ai quali perfino le Sezioni Unite della Cassazione hanno sostenuto che «è legittimo nutrire preoccupazioni per le accresciute potenzialità scrutatrici ed acquisitive dei virus informatici, suscettibili di ledere riservatezza, dignità e libertà delle persone», pur concludendo però che «è del pari legittimo ricordare che solo siffatti strumenti sono oggi in grado di penetrare canali criminali di comunicazione o di scambio di informazioni utilizzati per la commissione di gravissimi reati contro le persone»[43].

Più in generale, poi, appare abbastanza consolidata in Italia la deprecabile prassi di procedere ad intercettazione di soggetti indagati mentre si trovano assoggettati alla custodia cautelare in carcere, e di cui vengono captate conversazioni con altri detenuti (autentici o financo agenti sotto copertura) o addirittura con i propri familiari in sede di colloquio. Il tema non appare al centro della riflessione degli operatori o degli studiosi, che si sono al più concentrati sul tema delle intrusioni nella corrispondenza dei detenuti a seguito di una recente sentenza della Corte costituzionale[44], tuttavia meriterebbe a mio avviso ampia riflessione, all'insegna di una limitazione dell'impiego di questi strumenti tecnologici d'indagine nelle circostanze descritte: non si tratta evidentemente di una tecnologia nuova, ma io credo che il suo impiego rientri appieno nel catalogo che sto tracciando.

Da ultimo, merita ricordare anche quanto accadde nel caso Bossetti (nel quale, peraltro, fu fatto uso anche dell'intercettazione del colloquio in carcere dell'indagato con la moglie): in questo caso, gli strumenti tecnologici furono impiegati per condurre un

[41] Naturalmente, mi riferisco in particolare alla cosiddetta *Taricco II*: CGUE, C-42/17 – *M.A.S. and M.B.* (2017).

[42] Legge 9 gennaio 2019, n. 3, recante "Misure per il contrasto dei reati contro la pubblica amministrazione e in materia di trasparenza dei partiti e movimenti politici".

[43] Cass. civ., sez. un. 1° luglio 2016, n. 26889.

[44] D. Coduti, *La Corte costituzionale non dà il suo avallo alle "intercettazioni" della corrispondenza epistolare dei detenuti ma non esclude futuri sviluppi*, in *questa Rivista,* 1, 2017, 156 ss.; il riferimento è alla sentenza 24 gennaio 2017, n. 20.

vastissimo screening a tappeto di un'intera popolazione abitante in una determinata area, per poi procedere con l'inganno all'acquisizione di campioni di DNA, sotto il pretesto di un controllo del tasso alcolemico. Quella vicenda, che ha riempito le cronache dei quotidiani italiani, solleva certamente molti dubbi su quale sia il corretto bilanciamento da effettuare tra esigenze investigative di ricerca della verità e dei mezzi di prova, da un lato, e garanzie individuali, dall'altro, alla luce della disponibilità in capo agli investigatori di strumenti tecnologici molto invasivi; sul piano giudiziario, in ogni caso, tali modalità di indagine non solo state messe in alcun modo in discussione dalla magistratura[45].

Muovendo a considerare altri ordinamenti, vorrei ricordare un recente caso finlandese, che consente di allargare il discorso, ricollegandoci anche ad alcuni temi affrontati nelle pagine precedenti[46]. Si tratta della proposta, ad opera di un disegno legge di iniziativa governativa (HE 202/2017 vp), di attribuire alle agenzie di intelligenze militari e civili il potere di controllare le comunicazioni dei cittadini, senza dover dimostrare un nesso con uno specifico reato, in caso di semplice (e non meglio definita) minaccia alla sicurezza nazionale (e a certe condizioni anche in assenza di previa autorizzazione giurisdizionale). Per poter approvare la legge, il Parlamento provvide addirittura a modificare la costituzione, consentendo ad una legge ordinaria di limitare il diritto alla privacy per ragioni di sicurezza nazionale, se pur – anche per accogliere i rilievi del Comitato Costituzionale[47] – attenuando l'originaria proposta del governo di estendere l'applicazione dei nuovi poteri alla "prevenzione" di crimini, e limitandola così alla sola "investigazione" di crimini già commessi, nonché prevedendo che la minaccia alla sicurezza nazionale dovesse essere "seria" per giustificare le restrizioni. Pur con questi limiti, quindi, dopo una nuova pronuncia del Comitato Costituzionale[48], il disegno di legge 202/2017 fu definitivamente approvato. Questa vicenda è una poderosa testimonianza della tendenza del legislatore anche di ordinamenti ai vertici delle classifiche di qualità della democrazia a sfruttare le nuove tecnologie (anche se il tema, di per sé, predata naturalmente l'attuale rivoluzione tecnologica[49]) per estendere i poteri pubblici di sorveglianza al fine di contrastare terrorismo e altre minacce all'ordine pubblico, comprimendo le garanzie senza che la giustizia costituzionale riesca necessariamente a rappresentare un argine efficace[50].

---

45 Cass. pen., sez. I, 23 novembre 2018, n. 52872.

46 Cfr. il resoconto su I. Cameron, *Swedish report*, redatto nell'ambito del progetto di ricerca dello European Law Institute sulle *Common Constitutional Traditions in Europe*, inedito; v. anche il Comunicato stampa del Ministero della Giustizia finlandese, *Constitutional amendment concerning secrecy of confidential communications enters into force in October*, 4 ottobre 2018.

47 Rapporto del Comitato Costituzionale 4/2018 vp, 21 settembre 2018 sul disegno di legge costituzionale 198/2017 vp.

48 Opinione del Comitato Costituzionale 35/2018 vp, 15 novembre 2018.

49 Cfr. ad es. la sentenza della Corte europea dei diritti dell'uomo nel caso *Klass and Others c. Germania*, del 6 settembre 1978, ric. 5029/71, che già trattava il tema dei limiti costituzionali alla sorveglianza delle autorità di polizia, ben prima che gli strumenti informatici fornissero loro un nuovo potentissimo arsenale.

50 Una vicenda analoga si è invece conclusa con esito in parte diverso in Portogallo, dove la Corte costituzionale ha posto un argine al ripetuto tentativo legislativo di estendere i poteri di sorveglianza dei servizi di sicurezza di quello Stato: cfr. C. Santos Botelho, *Portuguese report*, redatto nell'ambito del

Questo ci porta a menzionare, se pur soltanto per brevissimi cenni, l'ordinamento dove maggiore è stata in anni recenti la riflessione su questi temi, ovvero gli Stati Uniti[51]. Patria della mastodontica operazione di sorveglianza su scala mondiale di Echelon[52], nonché dell'NSA, con le sue amplissime interferenze nelle comunicazioni private[53], e del *Patriot Act*, le cui disposizioni sulla raccolta di dati online e sulle telefonate sono state di recente prorogate ancora una volta nella propria validità da un accordo bipartisan che ha messo d'accordo due partiti su quasi ogni altra questione agli antipodi[54], gli Stati Uniti sono un fulgido esempio di democrazia compiuta che, di fronte a gravi minacce per la sicurezza nazionale, mette in atto misure straordinarie ed emergenziali, che però poi si protraggono per un tempo anche lunghissimo, comprimendo le garanzie, e incontrando limitati ostacoli sul piano giurisdizionale[55].

progetto di ricerca dello European Law Institute sulle *Common Constitutional Traditions in Europe*, inedito (sentenze 18 settembre 2019, n. 464, e 27 agosto 2015, n. 403). Un nuovo importante caso è quello promosso dall'Ombudsman di quel Paese a valle della notissima sentenza *Digital Rights Ireland* della Corte di giustizia dell'UE nelle cause riunite C-293/12 e C-594/12 (2014); con riguardo alla legislazione portoghese sulla data retention: cfr. E. Santos, Associação D3 – Defesa dos Direitos Digitais, Portugal, *Portugal: Data retention complaint reaches the Constitutional Court*, in *EDRi*, 25 settembre 2019. In ambito UE, oltre appunto a *Digital Rights Ireland*, va ricordata nella stessa direzione quanto meno *Tele2 Sverige AB*, cause riunite C-203/15 e C-698/15 (2016).

In argomento merita ricordare anche la situazione del Regno Unito. Nelle parole di C. O'Cinneide-D. Lock, *UK report* (redatto nell'ambito del medesimo progetto ELI), «*Recently the UK Government passed the Investigatory Powers Act 2016 which legal entrenched powers of bulk interception of communications carried out online. Bulk interception of internet communications, as well as a number of other types of bulk surveillance related to internet communications including bulk equipment interference (hacking), may be carried out by the UK Government. This surveillance can be carried out for a number of different purposes including to protect national security and if the 'main purpose' of the surveillance is collect 'overseas communications'. In reality much of the UK's internet communications carried out within the UK may be collected using bulk surveillance, due to the inability to distinguish between overseas and internal communications. These powers therefore have implications for freedom of expression in the UK. The issue is currently being decided upon by the Grand Chamber in Strasbourg in the case of* Big Brother Watch v UK»: si tratta di un caso da monitorare attentamente.

Fuori dall'Europa, di recente la High Court del Sudafrica della (Gauteng Division) ha stabilito l'incostituzionalità di molte disposizioni della articolata legge sulla sorveglianza del 2002 (*Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002*): sentenza 16 settembre 2019, *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* [2019] ZAGPPHC 384.

[51] Cfr. fra tanti, D. Gray, *The Fourth Amendment in an Age of Surveillance*, Cambridge, 2017.

[52] Cfr. P.R. Keefe, *Chatter: Uncovering the Echelon Surveillance Network and the Secret World of Global Eavesdropping*, New York, 2005; per i riflessi sull'Europa, v. K.J. Lawner, *Post-Sept. 11th International Surveillance Activity - A Failure of Intelligence: The Echelon Interception System & (and) the Fundamental Right to Privacy in Europe*, in *Pace Int'l L. Rev.,* 14, 2002, 435 ss.

[53] Cfr. G. Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*, London, 2015. A proposito di intercettazioni, una vicenda significativa è stata quella riferita poco oltre, alla nota 55 (order del 17 dicembre 2019).

[54] E. Boehm, *Congress Will Vote Today on Continuing Resolution That Hikes Spending, Extends Patriot Act Surveillance*, Reason, 19 novembre 2019. A onor del vero, a questa linea di tendenza fa da contraltare la giurisprudenza che ha tenuto ferme le garanzie (pur non in ambito tecnologico, dunque non rilevanti ai nostri fini), per i detenuti nell'ambito della guerra al terrorismo: v. *Rasul v. Bush*, *Hamdi v. Rumsfeld*, *Hamdan v. Rumsfeld*, e soprattutto *Boumediene v. Bush*.

[55] Al di là delle sentenze ricordate alla nota precedente, si possono ricordare i procedimenti civili e penali avviati (e talora già conclusisi con condanne pesantissime) nei confronti di Snowden, Manning, Assange: per un quadro molto approfondito, benché inevitabilmente non aggiornato con gli sviluppi più recenti, v. M.B. Kwoka, *Leaking and Legitimacy*, in *UC Davis Law Review,* 48, 2015, 1387 ss.).

Un caso in cui i giudici hanno posto un argine alla condotta delle autorità è stato quello che ha riguardato

Negli Stati Uniti si è poi anche sviluppato il tema molto interessante dei poteri di indagine delle autorità di polizia con riguardo ai cellulari protetti da password di criminali coinvolti in gravi reati e morti in conseguenza dei medesimi, l'accesso ai cui account informatici avrebbe consentito di aiutare le investigazioni. La vicenda fu come noto al centro di una disputa giudiziaria tra l'FBI e la Apple, con la seconda che si rifiutava di collaborare con la prima nello sbloccare i dispositivi altrimenti apparentemente inaccessibili dei criminali defunti, ed era determinata a contestare un primo ordine giudiziario di collaborare con il Bureau[56]. Il procedimento è stato poi archiviato dopo che l'FBI ha trovato la collaborazione di un soggetto che è riuscito a entrare negli iPhone in questione senza la collaborazione di Apple, tuttavia il tema si è riproposto di recente[57] e sarebbe molto interessante conoscere l'esito di analoga controversia qualora raggiungesse la Corte Suprema federale.

Un tema collegato e anch'esso di grande interesse è poi quello della possibilità o meno di imporre a persone indagate (in questo caso vive) di digitare la password di accesso ad un proprio dispositivo per consentire alle autorità investigative di accedervi: in casi come questi, alcune corti americane hanno ritenuto che l'imposizione di tale ordine non contrastasse con il privilegio contro l'autoincriminazione[58], mentre altre hanno ritenuto operante in questo caso la protezione costituzionale[59], per cui si tratta anche

l'ascolto delle conversazioni di un ex collaboratore di Trump, che era stato compiuto sulla base di informazioni rivelatesi infondate e con modalità non imparziali. In un order del 17 dicembre 2019, il giudice Collyer della Foreign Intelligence Surveillance Court ha rilevato che «*[t]he frequency with which representations made by FBI personnel turned out to be unsupported or contradicted by information in their possession, and with which they withheld information detrimental to their case, calls into question whether information contained in other FBI applications is reliable. The FISC expects the government to provide complete and accurate information in every filing with the Court. Without it, the FISC cannot properly ensure that the government conducts electronic surveillance for foreign intelligence purposes only when there is a sufficient factual basis*», ordinando quindi «*that the government shall, no later than January 10 2020, inform the Court in a sworn written submission of what it has done, and plans to do, to ensure that the statement of facts in each FBI application accurately and completely reflect*».

Un altro caso da ricordare è poi quello in cui il giudice federale Trenga ha stabilito, con un order del 4 settembre 2019, l'incostituzionalità del database di sospetti terroristi impiegato da FBI e Homeland Security Department nella lotta al terrorismo.

L'entità della sorveglianza messa in atto dall'FBI è al centro di una battaglia a colpi di richieste d'accesso, con conseguente risolto giurisdizionale, da parte del think tank libertario Cato Institute: cfr. il resoconto di P.G. Eddington, *How Extensive Is FBI Domestic Spying? We're Trying To Find Out*, in *Cato at Liberty*, 7 gennaio 2020.

Un ambito in cui, invece, sia la legislazione sia le corti non sono ancora intervenute, ma che acquisterà sempre maggior rilievo, è quello dell'accesso diretto delle forze di polizia ai dati registrati dalle società di sorveglianza con le telecamere installate per la sicurezza, condivisi da queste ultime con le forze dell'ordine spontaneamente (in modo non dissimile da quanto fatto da Clearview AI, su cui v. sopra, nota 27), così bypassando la necessità di un *search warrant*: cfr. D. McCullagh, *Doorbell Surveillance Networks Have Arrived. Should We Be Scared?*, in *Reason*, dicembre 2019.

[56] United States District Court for the Central District of California, No. ED 15-0451M, 16 febbraio 2016, in the matter of the search of an Apple iPhone seized during the execution of a search warrant on a black Lexus IS300, California License Plate 35KGD20

[57] Cfr. K. Benner, *Barr Asks Apple to Unlock Pensacola Killer's Phones, Setting Up Clash*, in *New York Times*, 13 gennaio 2020.

[58] Court of Appeals of the State of Oregon, *State v. Pittman*, 16 ottobre 2019, No. 466 (300 Or. App. 147, Or. Ct. App. 2019). Alle pagine 158 e seguenti, la sentenza contiene un'utile disamina giurisprudenziale sul tema.

[59] District Court of Appeal of the State of Florida, *G.A.Q.L. v. State of Florida*, 24 ottobre 2018, No. 4D18-1811; Court of Appeals of Indiana, *Katelin Eunjoo Seo v. State of Indana*, 21 agosto 2018, No.

in questo caso di un tema che andrà attentamente monitorato, in attesa di un possibile pronunciamento della Corte Suprema.

6. Conclusione: le ragioni di un costituzionalismo 1.0 di fronte alle sfide del *surveillance state*

Proprio l'ultima vicenda cui ho fatto cenno al termine del paragrafo precedente io credo confermi quanto ho sostenuto nella mia premessa più in alto, ovvero che la minaccia alle libertà individuali derivante da un impiego illiberale delle possibilità offerte dalle nuove tecnologie appare poter essere portata in modo assai più serio dalle autorità pubbliche rispetto alle grandi corporation, che invece – proprio come nel caso citato – possono tranquillamente svolgere addirittura la funzione opposta, di ultimi baluardi delle garanzie individuali, contro le minacce apportate dai pubblici poteri.
Ritengo quindi che il quadro delineato, per quanto inevitabilmente per sommi capi, metta ben in rilievo la tendenza in atto alla realizzazione di molte componenti del *surveillance state*. Come detto, i rischi di tale prospettiva appaiono molteplici, e di gran lunga superiori ai rischi del *surveillance capitalism*, che fino a prova contraria mantiene in capo a chiunque la libertà di sottrarsi alla raccolta di dati personali, purché si abbia un po' di accortezza nel proprio operato online e si sia disposti a rinunciare ad una serie di servizi sin qui offerti gratuitamente dalle grandi piattaforme.
Di fronte a questa prospettiva, io credo sia quanto mai urgente riaffermare le ragioni delle garanzie, e in definitiva quelle del costituzionalismo delle origini, ovvero un tentativo di predeterminare i confini del potere, arginandone l'operato tramite una previa definizione dei suoi limiti e una previsione di rimedi quanto più possibile efficaci in caso di travalicamento di tali limiti. Le nuove tecnologie non devono quindi necessariamente condurre a nulla di nuovo[60], e tantomeno ad un costituzionalismo 4.0[61], ma piuttosto appare più urgente riaffermare l'attualità del costituzionalismo di prima ondata, con il suo chiaro obiettivo, evidente sin dai testi più risalenti, di confinare il potere entro binari di operatività ben precisi e rispettosi dei diritti di libertà[62].
Il fatto che la tecnica renda possibile il perseguimento di determinati obiettivi non rende tale strada desiderabile se ciò avviene al costo di profonde (e per molti versi, questo sì, inedite) restrizioni delle libertà individuali. Solo la riaffermazione delle ragioni originarie del costituzionalismo e dei diritti fondamentali potrà infatti costituire un argine alla realizzazione di quel panopticon o grande fratello che potrà anche avere, in pro-

29A05-1710-CR-2466.

[60] Cfr. G. Inguscio, *Le* Lettere dal lago di Como *di Romano Guardini. Contenuto, evoluzione e aperture di un'opera dedicata al rapporto uomo-tecnica*, in *MondoDomani* (ringrazio la Prof.ssa Tania Groppi per lo spunto fornito in occasione del panel ricordato nella nota introduttiva).

[61] L'espressione *Constitutionalism 3.0* è stata usata da A. Somek come sottotitolo della *Introduction* al suo *The Cosmopolitan Constitution*, Oxford, 2014. È stata poi ripresa tra gli altri, anche con la variante 4.0 (pur, in entrambi i casi, con significati non del tutto coincidenti), da C. Corradetti-G. Sartor (a cura di), *Global Constitutionalism without Global Democracy?*, EUI Working Paper LAW 2016/21.

[62] Cfr. la lezione di N. Matteucci, *Breve storia del costituzionalismo*, Brescia, 2010; v. anche C. McIlwain, *Costituzionalismo antico e moderno*, Bologna, 1990 [1940].

spettiva utilitaristica, alcuni vantaggi, ma con troppi rischi per la libertà: e se, come in un noto aforisma, *il prezzo per quest'ultima è un'eterna vigilanza*[63], essa va esercitata anche vigilando nei confronti di chi vorrebbe sorvegliare "*le vite degli altri*"[64] troppo da vicino.

[63] Così il noto aforisma di Thomas Jefferson, ripreso nel titolo dell'omonimo libro di Dario Antiseri, Napoli, 2017.

[64] Il riferimento è al titolo di un celebre film sui distopici poteri di sorveglianza della Stasi.