Beni comuni nell'età della rimaterializzazione. Internet delle Cose fra apertura e resistenza collettiva

Guido NOTO LA DIEGA*

«This is not capitalism anymore; it is something worse.
The dominant ruling class of our time no longer maintains its rule through the ownership of the means of production as capitalists do. Nor through the ownership of land as landlords do. The dominant ruling class of our time owns and controls information»
McKenzie Wark, *Capital is dead* (Verso 2019) 10

Abstract: *The Internet of Things (IoT) heralds an era of unprecedented opportunities for capitalists to deploy new extractive practices leading to a third enclosure of the commons. The reason for that is what we call 'rematerialisation', namely the incorporation of immaterial goods (software, data, digital contents, even services) into material ones, which gives rise to a new category of hybrid good: the 'smart' device. As the world – including its most private spaces i.e., the home and the body – become embedded with sensors and actuators, IoT companies can extend their techno-legal power (stemming from a combination of contracts, Intellectual Property Rights (IPRs), technological protection measures, and factual controls) to each component of our 'smart' devices and systems. Knowledge being a commons, these powers lead to a tragedy of the anti-commons well illustrated by the transformation of our entire existence into data flows that are appropriated, re-used, and monetised by the 'smart' capitalists. Against this backdrop, this article sets forth a strategy to counter this enclosure by relying on the commons in the twofold sense of openness and a movement revolving around collective practices of resistance.*

Keywords: Internet of Things, beni comuni, *open source*, resistenza collettiva, occupazioni, smart anticommons

1. Introduzione

L'Internet delle Cose (noto come IoT, dalla perifrasi *Internet of Things*) ha definitivamente provato di non essere un fenomeno transeunte. Dai bollitori agli occhiali passando da aerei e

* Professore Associato di Diritto della Proprietà Intellettuale e della Privacy, Università di Stirling; Componente dell'Expert Group on AI and Data in Education and Training, Commissione Europea; Direttore, Scottish Law and Innovation Network (SCOTLIN); Fellow, Centro Nexa su Internet & Società. Email: gn12@stir.ac.uk. Questo articolo costituisce per certi versi lo sviluppo di alcune idee che avevo tratteggiato nelle conclusioni del mio libro Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies (Routledge, in corso di pubblicazione). Sono grato ai referee per i loro consigli e a Isabel Trujillo Perez e Giulia Sajeva per l'invito a contribuire a questo fascicolo. Grazie anche agli organizzatori e ai partecipanti ad alcuni eventi a cui ho presentato versioni precedenti di questo scritto: Ciclo di Seminari dei Corsi di dottorato in Diritto e innovazione e in Scienze giuridiche (Università di Macerata, 9 Aprile 2021); PGR Summer School «Owning the Land: from Private Property to Commons» (Università degli Studi di Palermo & Strathclyde University, Palermo, 17 Giugno 2021); Ciclo di seminari «Corso di diritto privato dell'informatica» (UnitelmaSapienza-JODI-TOELI, 3 Marzo 2022). Quest'articolo ha tratto giovamento da conversazioni con molti colleghi e amici; sono particolarmente grato a Salvatore Orlando, Daniele Imbruglia, Ermanno Calzolaio, Sirio Zolea, Shaira Thobani, Rowan Cruft, Tommaso Fia e Marco Brigaglia.

microinfusori insulinici, ogni *cosa* viene arricchita da sensori e capacità di connessione internet. Le montagne di dati generati da o mediante dispositivi *smart* potrebbero beneficiare gli utenti, le collettività di riferimento e la società più in generale. In questo senso, le spinte a considerare i dati come bene comune *extra commercium* vanno senz'altro accolte[1]. La realtà dell'IoT sembra però essere di segno opposto. Una realtà di espropriazione dei dati *smart*, in cui le società dell'IoT difendono rendite di posizione tramite monopoli sui dati che stanno conducendo a una tragedia degli *smart anticommons*.

Questo contributo intende gettare luce su detta tragedia e suggerire che il paradigma dei beni comuni possa aiutarci a cambiare il corso dell'IoT in una direzione socialmente utile. Il binomio IoT-beni comuni sarà osservato da due specole: apertura della conoscenza e pratiche collettive di resistenza. Storicamente, queste ultime hanno riguardato cose (beni tangibili come teatri, parchi, ecc.) piuttosto che risorse intangibili (conoscenza, internet)[2]. L'IoT supera i confini tradizionali tra materiale e immateriale, in quanto i dispositivi *smart* costituiscono un amalgama di hardware, software, servizi, contenuti digitali e dati. In questo senso parlo di rimaterializzazione dell'immateriale, un cambio di stato uguale e contrario alla digitalizzazione che da anni occupa la riflessione giuridica. La rimaterializzazione – software, servizi, contenuti digitali e dati vieppiù incorporati in prodotti fisici – costituisce un'opportunità senza precedenti per estendere il conflitto dal mondo delle cose a quello dell'Internet (delle Cose).

2. Rimaterializzazione, terza *enclosure* e tragedia degli *smart anticommons*

Da oltre un secolo, i civilisti si affannano a riflettere sui limiti dell'estensione di regimi concepiti per una realtà tangibile e analogica ad una immateriale e digitale.[3] La recente moda dei *non-fungible tokens* (NFTs) conferma che le questioni della smaterializzazione, digitalizzazione e tokenizzazione dei beni, lungi dall'essere transeunti, meritano di mantenere un ruolo centrale nella riflessione giuridica.

In tal senso, l'ascesa dell'IoT non segna il declino dell'inesausto dibattito sulle sfide dell'immateriale al diritto, sibbene illumina una nuova fase di sviluppo del capitalismo che si basa, ad un tempo, sulla trasformazione dell'interezza delle nostre vite in flussi di dati, e sull'estrazione di valore dagli stessi tramite pratiche che agiscono sul mondo nella sua dimensione tangibile. La trasformazione in dati avviene grazie a sensori (GPS, microfoni, ecc.), mentre «attuatori» utilizzano quei dati per agire sulla realtà fisica, ad es. se il sensore di umidità in un campo di grano segnala carenze d'acqua, le pompe di irrigazione si attiveranno automaticamente; o se l'algoritmo di Ikea determina il licenziamento di un'impiegata perché qualifica il ritardo (causato dal dovere accompagnare il figlio disabile a una visita medica) come mancanza di produttività[4]. Il capitalismo «smart» si agglutina attorno alla espropriazione

[1] Angiolini 2020.

[2] Esistono movimenti a livello sia italiano che internazionale che costituiscono voci importanti nel campo dell'apertura e socializzazione di conoscenza, internet, ecc. (si pensi alle meritorie attività dell'Associazione per la Scienza Aperta e della Right to Research Coalition). Questi movimenti non hanno ancora raggiunto la portata eversiva ed extra-accademica di movimenti benecomunisti sviluppatisi attorno a risorse fisiche, dai No Tav ai No Muos.

[3] Sul dibattito si veda la ricostruzione di Caterina 2010:385.

[4] della Ratta *et al.* 2018.

e monopolizzazione dei dati (*digital dispossession*)[5] e ad a un nuovo concetto di bene. Mentre sulla questione dei dati esiste un profluvio di contributi,[6] la principale sfida euristica dell'IoT consiste nel comprendere la natura non-binaria del bene *smart*, che rifugge la dicotomia materiale-immateriale e ci costringe a ripensare il bene non come categoria, sibbene come uno spettro fluido: in un mondo di dispositivi, sistemi e infrastrutture *smart*, fra i poli opposti del materiale e dell'immateriale vi sono la maggior parte dei beni che esibiscono, in misura variabile, tanto la materialità quanto l'immaterialità. A ben vedere, come è emerso in uno studio empirico sul termostato Nest di Google, i beni 'smart' sono una mescola inestricabile di hardware, software, dati, contenuti digitali e servizi[7].

Questa rimaterializzazione dei beni immateriali è una minaccia per il *knowledge commons* sistematizzato da Lin Ostrom e Charlotte Hess[8]. La minaccia della rimaterializzazione può essere facilmente compresa sol che si pensi alla differenza fra il libro e l'*e-book*. Una volta acquistato un libro, non vi sono limiti alle facoltà dominicali che possiamo esercitare sullo stesso e anche qualora intervengano dispute sui profili autoriali dello stesso, queste non avranno alcuna incidenza sulla proprietà del libro come *corpus mechanicum*. Questo perché l'acquisto della proprietà su un bene materiale tradizionale (non *smart*) crea una frattura non ricomponibile fra dante causa e avente causa. Per converso, il bene 'smart' consente al dante causa di mantenere il controllo sul bene potenzialmente *ad libitum*, certamente ben oltre il perfezionamento della compravendita o altra forma di trasferimento del diritto. È ben noto il caso degli utenti di Kindle, il lettore *e-book* di Amazon che, dopo aver acquistato *1984*, videro, dall'oggi al domani, scomparire gli e-book dai loro lettori a causa di una disputa autoriale riguardante gli stessi.

Nel mondo immateriale tradizionale, il dante cause mantiene il controllo sul bene post-vendita o sul servizio post-fornitura attraverso una combinazione di poteri fattuali e giuridici. I poteri fattuali includono (i) l'espropriazione dei dati e il controllo sugli stessi, con buona pace dei diritti dell'interessato a mente del Regolamento Generale sulla Protezione dei Dati Personali (GDPR);[9] (ii) la possibilità di fatto di interrompere il servizio, ad es. nel mondo del *software-as-a-service* il fornitore può unilateralmente e discrezionalmente escludere l'utente dal servizio qualora alleghi un utilizzo inaccettabile del servizio[10]; (iii) il potere tecnologico, classicamente illustrato dalla possibilità di sterilizzare le libere utilizzazioni nel diritto d'autore tramite misure tecnologiche di protezione[11] (ad es. il c.d. *upload filter* che obbliga piattaforme come YouTube a prevenire il caricamento di contenuti che vengano ritenuti in violazione del diritto d'autore)[12].

---

[5] Noto La Diega,Derclaye (forthcoming).

[6] V. ad es. Elvy 2021.

[7] Noto La Diega,Walden 2016.

[8] Hess,Ostrom, 2007.

[9] V. ad es. Noto La Diega,Sappa 2020, dove si discute della tensione fra segreti commerciali e tutela dei dati personali.

[10] Il SaaS non si vende, si concede in godimento temporaneo e non si scarica, sibbene si accede allo stesso sul cloud, con la relativa infrastruttura, middleware, software e dati che rimangono nel *data centre* del fornitore. V. Savelyev 2014.

[11] Su questa forma di *paracopyright*, forma di tutela ulteriore al *copyright* e foriera di eccessi proprietari, v. ad es. Westkamp 2010.

[12] Direttiva UE 2019/790 del Parlamento Europeo e del Consiglio del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (Direttiva Copyright Digitale) [2019] OJ L 130/92, art 17. In teoria – come reiterato in C-401/19 *Polonia c. Parlamento Europeo e Consiglio UE,* in *Guida al diritto*, 2022, 18 – i filtri dovrebbero tenere conto delle libere utilizzazioni, ma si dubita

Come suggerisce quest'ultimo punto, i poteri fattuali sono intimamente legati a quelli giuridici, ipostatizzati nell'esclusiva autoriale, la privativa industriale e i contratti. Per quanto concerne il potere esercitato tramite la c.d. proprietà intellettuale (PI), basti notare come nell'infosfera[13] sia possibile prevenire e contrastare comportamenti (di solito unilateralmente considerati come) illegali in modi impensabili e impraticabili nel mondo 'offline'. Quanto alla prevenzione, si pensi alle piattaforme blockchain che consentono di tracciare chi stia ascoltando la musica e che rendono il pagamento delle royalty e l'individuazione dei titolari assai più immediato dei metodi tradizionali[14]. Quanto alla repressione delle condotte in violazione della PI, i relativi titolari si possono agevolmente affidare alle piattaforme digitali affinché monitorino il traffico, eliminino i contenuti sospetti e puniscano gli utenti con sanzioni private (ad es. la cancellazione dell'account)[15]. Quanto ai poteri contrattuali, un esempio significativo è fornito dalla sentenza della Corte di Giustizia in *Ryanair v PR Aviation*[16]. In quel caso, la nota compagnia aerea *low cost,* nonostante non vantasse un diritto di PI sui dati relativi ai propri voli, poteva controllare l'uso di suddetti dati da parte di terzi per mezzo delle clausole *anti-scraping* nei termini d'uso del proprio sito[17].

In virtù della rimaterializzazione, i poteri fattuali e giuridici che tradizionalmente consentivano al dante causa del bene immateriale di mantenere il controllo sul bene indefinitamente, si estendono alla realtà tangibile, nel momento in cui quest'ultima incorpora uno o più elementi che la rendono *smart* (dati, software, ecc.). Josh Fairfield nel suo *Owned*[18] fa riferimento a un esempio che ben illustra gli effetti pratici di codesta estensione. Da qualche anno, il leader mondiale nel campo della produzione di trattori, John Deere, ha cominciato a sostituire i propri trattori analogici con equivalenti *smart*. Dopo un iniziale entusiasmo, gli agricoltori americani si resero conto che la natura *smart* dei loro nuovi trattori comportava la perdita del relativo *right to repair*. Infatti, ai sensi della licenza che accompagna il software incorporato nei trattori, la riparazione non autorizzata costituirebbe una violazione del diritto d'autore *sub specie* circonvenzione di una misura tecnologica di protezione. Il controllo sulle componenti immateriali del bene consente all'avente causa di mantenere il controllo sul bene *smart* nella sua totalità, comprese le componenti tangibili. E c'è di più. Non solo quei poteri fattuali e giuridici di cui sopra si estendono dall'immateriale al materiale, ma la situazione è financo peggiore a causa del cumulo di diritti PI che connota l'IoT. Siccome i dispositivi *smart* sono una mescola di hardware, software, dati, contenuti digitali e servizi – e siccome su ognuno di questi elementi (fatta eccezione per i servizi) insistono un ginepraio di diritti PI – le prerogative degli utenti dei dispositivi *smart* sono significativamente compresse da questo coacervo di *Immaterialgüterrechte*. Si pensi allo smartphone: con ogni probabilità, il sistema operativo sarà

che questo sia tecnicamente possibile (come tradurre in linguaggio binario concetti intrinsecamente vaghi come *fairness*?).

[13] Floridi 2020.

[14] Guochao *et al.* 2021. È anche vero che, una volta che il contenuto illegale si trova sulla blockchain può diventare impossibile rimuoverlo. Sulla relazione anfibola fra blockchain e violazione del diritto d'autore sia consentito il rinvio a Noto La Diega,Stacey, 2018.

[15] Trib. Bologna, sez. II, 10 Marzo 2021, in *GiustiziaCivile.com*, 13 Ottobre 2021 con nota di Scandola 2021, ha riconosciuto la risarcibilità del danno da rimozione di profilo *social*.

[16] *Guida al diritto*, 2015, 10, 105 (s.m).

[17] Monterossi 2020. Lo *scraping* è il processo di estrazione di dati da fonti digitali affinché' un programma per elaboratore possa replicarli, formattarli o modificarli in modo automatizzato (ad es. *web scraping*).

[18] Fairfield 2017.

protetto dal diritto, il design sarà tutelato ai sensi della disciplina dei disegni e modelli[19], sensori come wi-fi e Bluetooth saranno brevettati, gli algoritmi incorporati saranno oggetti di segreto industriale e altri aspetti come il logo rientreranno nella disciplina dei marchi. Il tutto è reso ancora più complesso dai potenziali conflitti di titolarità, come visto nel caso *Google LLC v Oracle America Inc*[20], riguardante l'inclusione nel sistema operativo Android di elementi dell'interfaccia Java e stringhe di codice di proprietà di Oracle.

Il combinato disposto dell'estensione del controllo giuridico e fattuale dall'immateriale all'immateriale e il cumulo di diritti di PI ha portato molti a denunciare la morte della proprietà nell'IoT[21]. Non spetta a me dire se la proprietà sia in effetti morta, per quanto la resilienza della stessa imporrebbe cautela, ma ciò che preme è di qualificare il fenomeno come una forma di terza *enclosure* o di tragedia degli *smart anticommons*. Nel «second enclosure movement»[22], gli steccati presero la forma della PI, grazie alla quale «things that were formerly thought of as common property, or as "uncommodifiable" or outside the market altogether, are being covered with new, or newly extended, property rights»[23]. I dati, o ai tempi si sarebbe detto l'informazione e la conoscenza, sono per loro natura un bene comune e costituisce una chiara scelta di politica del diritto quella di trattarli come proprietà[24]. Mentre l'espansione orizzontale e verticale della PI[25] dimostra che tanto a livello nazionale che internazionale i legislatori hanno ritenuto di incentivare la terza *enclosure*, l'avvento dell'IoT ha fornito gli strumenti tecnologici e fattuali per chiudere il cerchio.

Questo movimento può essere anche considerato come una forma di «tragedia degli *anticommons*». Questa categoria conoscitiva – nata in opposizione alla c.d. tragedia dei beni comuni[26] che vorrebbe giustificare la proprietà privata come un dispositivo che prevenga lo sfruttamento inefficiente dei beni comuni – fa luce sul fenomeno per cui eccessi proprietari conducono al sottoutilizzo delle risorse comuni. Mutuando Michael Heller, «(i)f too many owners control a single resource, cooperation breaks down, wealth disappears, and everybody loses»[27]. Ed è esattamente ciò che accade nell'IoT, dove a fronte della supposta proprietà del dispositivo *smart* da parte del consumatore, si affollano una folta schiera di titolari dei diritti di PI e diritti *de facto* proprietari sui dati[28].

Che la *propertization* dell'IoT costituisca una minaccia ai beni comuni diviene evidente sol che si pensi al potenziale benecomunista delle tecnologie *smart*[29]. Per ragioni di sintesi, si pensi allo studio della Nazioni Unite[30] che, nel perorare la causa del riutilizzo dei big data per il

[19] Codice della Proprietà Industriale, art. 31 ss.
[20] 593 U.S. ___ (2021).
[21] Fairfield 2017.
[22] Sulla prima *enclosure*, invece, una pietra miliare è costituita da Grossi 1977.
[23] Boyle 2010: 45.
[24] *International News Serv. v. Associated Press* 248 U.S. 215, 250 (1918).
[25] Nivarra 2007:498.
[26] La perifrasi si deve al notissimo articolo di Hardin, 1968, anche se la potente metafora dei pascoli in rovina viene da una lezione tenuta ad Oxford nel 1833 dal matematico William Foster Lloyd (v. Lloyd 1980). Entrambi gli interventi avevano a che fare con questioni diverse da quelle che poi occuparono i fautori della supposta tragedia dei beni comuni, cioè questioni di controllo della popolazione.
[27] Heller 2013: 6.
[28] Non intendo con ciò affrontare la questione teorica, pregna di conseguenze pratiche, della configurabilità di un diritto di proprietà sui dati. Cfr. Michels and Millard 2022.
[29] Sia consentito il rinvio a Noto La Diega,Derclaye (forthcoming).
[30] *Big Data for Sustainable Development*, 2020.

raggiungimento degli obiettivi di sviluppo sostenibile, esemplifica il collegamento fra dati e obiettivo facendo riferimento *inter alia* a:

(i) La connessione di sensori alle pompe idrauliche per tracciare l'accesso all'acqua (Obiettivo 3)[31];

(ii) L'uso di sensori satellitari per monitorare da remoto gli sconfinamenti in spazi pubblici, parchi, ecc. (Obiettivo 11)[32];

(iii) La combinazione di dati aperti, testimonianze *crowd-sourced* e immagini satellitari per contrastare la deforestazione (Obiettivo 13)[33];

Se vogliamo che le tecnologie *smart* usino i big data per il bene comune è fondamentale che i dati vengono trattati come bene comune (*open data*) piuttosto che come oggetto di proprietà. Un esempio che mi pare illustrativo di questo postulato è fornito dallo European Tracking Network, che usa sensori aperti (*fish tags*) e dati aperti per integrare tutti i sistemi di tracciamento all'interno di un'unica rete europea. Se i sensori e i dati fossero 'enclosed' o proprietari la condivisione delle informazioni e l'integrazione dei sistemi non sarebbe realizzabile.

Gli abusi proprietari sottesi a «morte della proprietà», «terza enclosure» e «tragedy of the smart anticommons» sono in antitesi ai beni comuni perché ruotano attorno alla monopolizzazione dei dati e a sistemi chiusi che costituiscono ostacoli al porre l'IoT al servizio del bene comune.

3. Beni comuni e IoT aperto

Siamo ancora in tempo per cambiare il corso del mondo *smart* in una direzione benecomunista. Il rapporto fra beni comuni e nuove tecnologie è anfibolo. Da una parte, abbondano le soluzioni tecnologiche ai problemi relativi alla gestione di risorse naturali e immateriali di cui la collettività può beneficiare. Dall'altra, le tecnologie emergenti possono rendere i beni comuni più vulnerabili grazie al loro potenziale di «capture the previously uncapturable»[34].

Questo contributo non aspira a ricondurre a sistema i beni comuni, concetto intrinsecamente polisemico[35]. Più modestamente, intende riflettere sull'adozione dei beni comuni come strumento per mettere l'IoT al servizio della società. A tal fine, il binomio IoT e beni comuni è analizzato attraverso un duplice prisma. In primo luogo, mi occuperò di beni comuni nel senso di tecnologie 'aperte'. L'*open access* (accesso aperto) costituisce il nocciolo duro della conoscenza come bene comune[36]. Il riferimento più immediato è al *Free/Libre Open Source Software* (F/LOSS) e ai *creative commons* come strumento per la scienza aperta. La seconda accezione di beni comuni – cui dedicherò il prossimo paragrafo – riguarda un uso antagonistico dei medesimi come punti di emersione di forme di resistenza collettiva extragiuridica[37].

L'*openness* è essenziale nell'IoT per un duplice motivo. Da una parte, se si affermassero modelli chiusi e proprietari questi stenterebbero a parlarsi l'un l'altro (a essere interoperabili) il che condurrebbe a dispositivi e sistemi isolati e non comunicanti. Accanto a questo motivo

[31] UN Sustainable Development Goal (SDG) 6: Acqua Pulita e Servizi Igienico-Sanitari.
[32] SDG 11: Città e comunità sostenibili.
[33] SDG 13: Lotta contro il cambiamento climatico.
[34] Hess, Ostrom 2007: 10.
[35] Su quattro dei significati di 'bene comune' v. Nivarra 2016.
[36] Ghosh 2007: 210.
[37] Millner-Larsen, Butt: 2018.

ontologico, ve n'è uno politico. Se vogliamo che l'IoT diventi una realtà di cui i cittadini si possano fidare, lo stesso deve diventare trasparente e il suo codice modificabile e riutilizzabile per riflettere i bisogni delle collettività di riferimento. Affinché la coppia beni comuni-IoT aperto possa esprimere il proprio potenziale trasformativo è necessario: (i) riflettere criticamente sul concetto di F/LOSS; (ii) comprendere che, se i dispositivi *smart* sono un amalgama di software, hardware, ecc., diventa cruciale che ogni componente risulti aperta.

Il F/LOSS ha due elementi fondamentali: la libertà (di usare, copiare, studiare e modificare il programma) e l'apertura (il codice sorgente è condiviso in modo tale che gli utenti possano ispezionarlo e che siano incentivati a migliorarle il design). Si commetterebbe un errore qualora si ritenesse che F/LOSS e *open source software* (OSS) siano perifrasi intercambiabili. Per dirla con Richard Stallman[38], il primo è un movimento sociale, il secondo una metodologia di sviluppo software. La differenza appare in tutto il suo nitore a chi noti come l'OSS sia stato appropriato dagli alfieri del software proprietario, cioè quel gruppo di multinazionali ad appartenenza variabile che per comodità possiamo chiamare *big tech* (Facebook, Tencent, ecc.). Basti pensare all'acquisizione di società F/LOSS, come fece IBM con Red Hat[39], o alla messa a disposizione di codice sorgente da parte di Meta[40], Google[41] e Microsoft[42]. Di là dalle intenzioni, detta appropriazione ha depoliticizzato il software aperto così sterilizzandone il potenziale eversivo.

Ciò posto, non si può affidare al F/LOSS la soluzione di tutti i problemi dell'IoT. Onde riflettere la natura ibrida del fenomeno in esame, è necessario esportare le logiche e pratiche di apertura ad altri aspetti e componenti dell'IoT, segnatamente l'hardware, le piattaforme e i dati.

L'apertura delle componenti hardware dei dispositivi *smart* si riferisce primariamente al concetto di brevetti aperti o *open patents*, tornati in auge durante la pandemia, dacché un coro di voci si alzava per far si che i vaccini potessero circolare e essere prodotti evitando le strozzature derivanti dalla privativa industriale[43]. Il fenomeno dei brevetti aperti resta di difficile comprensione giacché si riferisce a una realtà multiforme, per cui risulta utile riferirsi a un esempio concreto quale l'Open Invention Network[44]. Quest'ultimo si propone di raffinare il modello della PI affinché i brevetti possano essere condivisi apertamente (gratuitamente) in un ecosistema collaborativo in cui i partecipanti sono uniti dall'impegno di non esercitare le facoltà proprietarie connesse al brevetto. Per quanto codeste iniziative non siano più isolate e si possa financo dire che vi sia una proliferazione delle stesse[45], non si può negare che per lo più subiscano le medesime limitazioni dei tradizionali paradigmi brevettuali[46]. Un modello realmente aperto di hardware dovrebbe rifiutare in radice le logiche della PI, piuttosto che più

[38] Stallman 2022.
[39] *IBM Closes Landmark Acquisition of Red Hat for $34 Billion; Defines Open, Hybrid Cloud Future*, 2019.
[40] *Meta Open Source*, 2022.
[41] *Google Open Source*, 2022.
[42] *Microsoft Open Source*, 2022.
[43] Paradigmatico è il dibattito fra i proponenti del TRIPs *waiver* (sospensione temporanea dei diritti di PI) – su iniziativa di India e Sud Africa, poi appoggiato da oltre 100 paesi – e coloro che vi si oppongono (Regno Unito, UE e altri esponenti della c.d. civiltà occidentale). V., da una parte, Kang *et al.* 2021, una lettera fra i cui firmatari figura il sottoscritto e, dall'altra, Hilty *et al.* 2021. Una frattura che sembra senza precedenti e che segnala, a un tempo, la natura politica della PI e la capacità dei beni comuni di diventare luogo di emersione del conflitto.
[44] *Open Invention Network (OIN)*, 2022.
[45] Estèves 2018.
[46] Maggiolino,Montagnani 2011.

modestamente mirare a riformare il sistema dei brevetti. Il principale limite allo sviluppo di dispositivi e sistemi realmente aperti consiste nelle preoccupazioni attinenti alla sicurezza. Un esempio è fornito dal tentativo dell'Università di Edimburgo di rendere *smart* il proprio campus. Un'iniziativa affatto meritoria e che ha incluso lo sforzo di rendere ogni hardware «component should ideally be accessible, modifiable and available for experimentation within the constraints of security concerns»[47]. Per quanto nell'IoT la sicurezza abbia acquistato un'importanza maggiore – si pensi a cosa accadrebbe se una pompa di benzina *smart* venisse hackerata – mi sembra che molto spesso solo una cieca adesione all'ideologia securitaria prevalente non consente di vedere come non vi debba essere un'incompatibilità ontologica fra *open source* e sicurezza[48].

In secondo luogo, dato che l'IoT è controllato da un novero ristretto di potenti piattaforme digitali, bisogna dire qualcosa su cosa voglia dire aprire le piattaforme. Il funzionamento degli algoritmi sottesi all'IoT è notoriamente descritto come una scatola nera, soprattutto quando incorporano i metodi dell'Intelligenza Artificiale (IA)[49]. La scatola nera indica l'impossibilità di determinare come il sistema sia giunto a una decisione B partendo dai dati di input A. Il ruolo delle piattaforme, però, richiama l'attenzione su un altro tipo di opacità, la cosiddetta scatola nera societaria o *organisational black box*, per cui le società che controllano gli algoritmi sono «private, profit-maximising entities, operating under minimal transparency obligations»[50]. Anche con l'obiettivo di contrastare codesta chiusura delle piattaforme, la Commissione Europea ha proposto una serie di misure rientranti nel quadro del mercato unico digitale.

È impossibile dar conto di tutti i frammenti che compongono il relativo quadro normativo, mi limiterò a rilevare un contrasto fra alcune previsioni atte a costringere le piattaforme ad aprirsi e altre che, invece, costituiscono un passo indietro. In positivo, cominciando con la proposta di legge europea sui servizi digitali (Digital Services Act)[51], si può notare un novero di obblighi di apertura come ad es. la produzione di rapporti sulle attività di moderazione dei contenuti condivisi dagli utenti[52], maggiore trasparenze circa i parametri usati nella pubblicità online[53] e, ciò che più conta, l'obbligo di aprirsi ad audit indipendenti[54]. Gli obblighi sono modulati a seconda del tipo di piattaforma; ad esempio, i primi gravano su tutti gli intermediari online[55], i secondi solo sulle piattaforme online[56], i terzi sulle piattaforme online di dimensioni molto grandi[57].

[47] Dominguez 2020 8.
[48] V. ad es. Wen, Kianpour, Kowalski 2019.
[49] Di qui, la *black box society* denunciata da Pasquale 2015.
[50] Perel, Elkin-Koren 2017: 181.
[51] Proposta di Regolamento del Parlamento Europea e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE (DSA) (COM/2020/825 final).
[52] DSA, art. 13.
[53] DSA, art. 24.
[54] DSA, art. 28.
[55] DSA, art 2, lett. f); il riferimento è a hosting, caching e mere conduit, *safe harbours* ai sensi della Direttiva e-Commerce.
[56] DSA, art. 2, lett h).
[57] DSA, art. 25(1).

La proposta di legge sui mercati digitali (Digital Markets Act)[58], dal canto suo, si concentra su un tipo di piattaforma chiamata *gatekeeper*[59] che è chiamata a sottoporre a audit indipendenti le proprie tecniche di profilazione dei consumatori[60], a fornire agli utenti commerciali accesso a dati aggregati e non aggregati[61] e ai fornitori terzi di motori di ricerca online l'accesso ai dati relativi a posizionamento, ricerca, click e visualizzazione per quanto concerne le ricerche effettuate dagli utenti finali sui motori di ricerca online del *gatekeeper*[62]. Infine, la famigerata proposta di legge europea sull'IA (AI Act)[63] a mente della quale i fornitori di sistemi IA ad alto rischio dovranno aprirsi alle ispezioni delle autorità di sorveglianza del mercato e garantire l'accesso ai dati di addestramento, convalida e prova utilizzati dal fornitore, incluso in certe circostanze l'accesso al codice sorgente del sistema di IA[64].

Allo stesso tempo, l'attuale (e proposta) regolazione delle piattaforme può condurre ad atteggiamenti di chiusura per almeno due motivi. In primo luogo, è diventata una prassi costante nella produzione giuridica europea in tema di piattaforme l'inclusione di clausole di salvaguardia che fan sì che le piattaforme possano invocare la PI come scudo a ogni tentativo di apertura. Esula da questo contributo una rassegna di dette clausole, basti pensare che le piattaforme molto grandi non possono essere obbligate a fornire al coordinatore dei servizi digitali del luogo di stabilimento o alla Commissione l'accesso ai dati necessari per monitorare la conformità al Digital Services Act quando «dare accesso ai dati comporterebbe notevoli vulnerabilità […] per la protezione delle informazioni riservate, in particolare dei segreti commerciali»[65]. In secondo luogo, l'incremento degli obblighi gravanti sulle piattaforme[66] è problematico perché è facile prevedere che onde ottemperare le piattaforme dovranno di fatto divenire proattive nel sorvegliare i propri utenti e ragioni economiche e strategiche costituiranno incentivo affinché detta sorveglianze avvenga con modalità algoritmiche (e quindi intrinsecamente opache). Illustrativo in tal senso è il c.d. *upload filter* introdotto dalla Direttiva sul Diritto d'Autore nel Mercato Unico Digitale[67]. I prestatori di servizi di

[58] Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali o DMA) (COM(2020) 842 final).

[59] Un *gatekeeper* è un fornitore di servizi di piattaforma di base (cloud, motori di ricerca, ecc.) avente un impatto significativo sul mercato interno, anche grazie al controllo su un punto di accesso importante affinché gli utenti commerciali raggiungano gli utenti finali e avente una posizione consolidata e duratura nell'ambito delle proprie attività o è prevedibile che acquisisca siffatta posizione nel prossimo futuro (DMA, artt. 2(1), 2(2), 3(1)).

[60] DMA, art. 13.

[61] DMA, art. 6(1)(i).

[62] DMA, art. 6(1)(j).

[63] Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale o AI Act) e modifica alcuni atti legislativi dell'Unione (COM(2021) 206 final).

[64] AI Act, art. 64(1)(2).

[65] DSA, art. 31(6)(b).

[66] Tradizionalmente, la regolazione delle piattaforme ruotava attorno al divieto di introdurre sistemi di monitoraggio indiscriminato del traffico online; a codesto divieto era collegato un ventaglio di esenzioni o *safe harbours* per le piattaforme che non avevano conoscenza dei comportamenti illegali dei propri utenti o che, avendone ricevuto conoscenza, rimuovessero prontamente i relativi contenuti. Tanto la Direttiva e-Commerce in Europea quanto il Communications Decency Act e il Digital Millennium Copyright Act negli Stati Uniti adottano questo approccio. Negli ultimi anni si è assistito a un'ascesa delle c.d. *monitoring obligations* per cui, mentre si ribadisce che, almeno in teoria, l'architettura della Direttiva e-Commerce resta intatta, di fatto si obbligano le piattaforme a sorvegliare i propri utenti in modi che sollevano dubbi dal punto di vista dei diritti umani alla riservatezza e alla libertà d'espressione. V. ad es. Frosio 2017.

[67] Direttiva Copyright Digitale, art. 17.

condivisione di contenuti online saranno direttamente responsabili per le violazioni del diritto d'autore commesse dai propri utenti qualora non abbiano posto in essere i massimi sforzi per prevenire che gli utenti possano caricare contenuti di tal fatta[68]. Un'aggiudicazione lasciata a un soggetto privato e imparziale il quale è ragionevole attendersi dovrà adottare sistemi algoritmici di sorveglianza – inscrutabili scatole nere – in barba alla riservatezza, la libertà d'espressione e la supposta apertura delle piattaforme[69].

Un altro elemento che necessita apertura affinché l'IoT nella sua interezza diventi aperto sono i dati, ai quali si dedicherà meno spazio giacché sugli *open data* si sono versati i proverbiali fiumi d'inchiostro[70]. Come uno degli stakeholder dell'IoT che ho intervistato per un'altra ricerca, «open data is vital as the long-term impact of IoT data is unimaginable»[71]. L'impatto sulla società dell'uso (e riuso) dei dati generati da e mediante dispositivi smart è imprevedibile e la trasparenza, portabilità e riutilizzabilità degli *open data* concorre a garantire un maggiore controllo sull'uso responsabile delle tecnologie dell'IoT. E senza dati aperti non sarebbero possibili molte delle applicazioni *smart* che negli ultimi anni sono state sviluppate per il bene comune. Ad esempio, grazie a dati aperti e hardware aperto, lo European Tracking Network è riuscito a integrare in un solo network a livello europeo il tracciamento degli animali acquatici[72]. Storicamente, i dati aperti sono stati appannaggio degli amministrativisti[73], una conseguenza naturale dal profluvio di atti normativi che, a ogni livello, hanno via via forzato la pubblica amministrazione ad allentare le maglie del controllo sui propri documenti e dati[74]. Negli ultimi anni, soprattutto su spinta del legislatore UE, una serie di provvedimenti sono stati adottati affinché anche i dati dei privati divengano aperti, portabili, riutilizzabili, condivisibili[75]. Per quel che qui rileva[76], basti riferirsi al più recente dei pilastri della strategia europea di regolazione dell'economia dei dati, segnatamente il Regolamento sulla Governance dei Dati (*Data Governance Act* o DGA)[77]. il DGA ruota attorno al concetto di altruismo dei dati, una sorta di imperativo morale per cui i cittadini sono invitati a condividere gratuitamente

[68] Legge 22 aprile 1941, n. 633 (legge sul diritto d'autore o l. aut.), art. 102-*septies*.

[69] La Corte di Giustizia UE ha sancito che l'art. 17 della Direttiva Copyright Digitale contiene sufficienti garanzie a tutela della libertà d'espressione (*Polonia c. Parlamento Europeo*). Duole che la Corte non abbia debitamente considerato la rilevanza della 'chiusura' e opacità dell'upload filter che hanno un impatto sulla determinazione della questione in esame. Cfr. Geiger, Jütte 2022.

[70] Per uno studio sistematico dei dati aperti v. Aliprandi 2014.

[71] Noto La Diega 2022.

[72] Jan *et al.* 2018.

[73] Non sono mancate però altre prospettive ad es. di informatica giuridica (Palmirani *et al.*, 2018), diritto d'autore (Sappa, 2021) e diritto privato comparato (Caso 2022).

[74] V. ad es. la Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (Direttiva Open Data) [2019] OJ L 172/56.

[75] Sarebbe impossibile, data la sede, dar conto di tutti gli strumenti *de quibus.* Oltre a quelli riferiti nel corpo di quest'articolo, basti pensare alla portabilità dei dati personali ai sensi del Regolamento Privacy (GDPR), dei dati non-personali (Regolamento sulla Libera Circolazione dei Dati Non Personali) e la portabilità dei servizi (Regolamento sulla Portabilità Transfrontaliera di Servizi di Contenuti Online). V. Borghi 2018; Montagnani 2019; Karmel 2020; Fia 2021.

[76] Rileva pure la Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (Normativa sui Dati o *Data Act*) (COM(2022) 68 final) su cui sorvolerò per ragioni di sintesi; mi sia consentito sul punto rinviare a Noto La Diega, Derclaye (forthcoming).

[77] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati o DGA) [2022] OJ L 152/1.

i propri dati personali per obiettivi di interesse generale[78]. Da una parte, va salutato con favore il tentativo di superare le concezioni proprietarie dei dati scaturite da letture cursorie del Regolamento Privacy[79] e abbracciare, invece, l'idea che i nostri dati possano essere usati per il bene comune, ad es. a fini di «assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità»[80]. Dall'altra parte, almeno tre ordini di critiche possono essere mossi al DGA. In primo luogo, l'utilizzo del termine 'altruismo' contiene un giudizio di valore per cui, qualora i cittadini decidano di non condividere i propri dati debbano essere tacciati di egoismo, mentre vi possono essere motivi più che legittimi di non aprire i propri dati personali al riuso (ad es. la consapevolezza che questi possano essere usati a fini discriminatori). In secondo luogo, l'altruismo dei dati potrebbe essere strumentalizzato dalle imprese IoT-capitalisti della sorveglianza *à la* Zuboff[81] che espropriano e monopolizzano i nostri dati grazie ai congegni retorici del *data waste* e *dark data*[82]. Il ragionamento, in breve, è il seguente: per il fatto stesso di esistere, produciamo quotidianamente grandi quantità di dati che, se non venissero sfruttati, andrebbero sprecati; questi dati sono, per così dire, neri in quanto restano nell'oscurità e il loro mancato sfruttano non consentirebbe alle imprese IoT di essere efficienti e creative. La suddetta espropriazione dei dati, allora, viene presentata come servizio di cui cittadini-consumatori dovrebbero beneficiare perché, grazie alla perdita di controllo sui dati derivante dall'utilizzo di dispositivi *smart*, possono godere dei tanti e innovativi servizi che sfruttano la trasformazione della nostra vita in flussi strutturati di dati[83]. Il terzo ordine di critiche attiene al modello di governance proposto dal DGA, a ragione considerato individualistico anche nella misura in cui ignora gli interessi dei destinatari delle decisioni prese sulla base dei dati 'altruisticamente' donati[84]. Da qualche decennio ormai si è affermata l'idea che le tecnologie sono artefatti politici[85]. È venuto il momento di riconoscere che anche le preferenze circa la governance dei dati sono di natura politica, il che è un forte argomento a favore di approcci più partecipativi e incentrati non solo sugli individui ma anche sulle collettività e comunità di riferimento[86] – il che ci riporta ai beni comuni, sia pure nella seconda accezione di punto di agglutinamento per pratiche di resistenza collettiva, a cui è dedicato il prossimo paragrafo.

4. Beni comuni e pratiche di resistenza collettiva alle pratiche estrattive *smart*

Il collegamento fra beni comuni e dimensione collettiva è meno scontato di quanto non sembri. Un nesso ovvio si rinviene anche nella notissima definizione di beni comuni di cui al *DDL*

[78] DGA, art. 2(16).
[79] Sintomatiche in tal senso sono affermazioni come quelle per cui «laws like the GDPR are starting to more clearly define ownership (…) "data subjects" will always maintain ownership over any personal data they share with you» ('Who owns the personal data you collect from users?', 2020).
[80] DGA, art. 2(16).
[81] Zuboff 2019: 202.
[82] Glick 2016.
[83] V. *amplius* Noto La Diega 2022: cap. 5.
[84] Viljoen 2021.
[85] Winner 1980.
[86] Tennison 2020.

Rodotà[87]. L'essere a servizio immediato della collettività – che «in persona dei suoi componenti, della presente e delle future generazioni è ammessa istituzionalmente a goderne in modo diretto»[88] – ne era elemento definitorio centrale. Il DDL mostrava grande lungimiranza anche nell'emendare l'art. 810 c.c. per includere espressamente, nella definizione di bene giuridico tanto le cose materiali, quanto quelle immateriali, così potenzialmente contribuendo a rendere il nostro Codice civile *IoT-proof*. Nonostante la sua infelice sorte politica, il DDL resta un importante spunto per ogni riflessione sui beni comuni e, per quel che rileva ai fini di questo saggio, mi fornisce il punto di partenza per mettere a fuoco la dimensione collettiva e non-binaria dei beni comuni applicati all'IoT.

Un collegamento meno immediato fra beni comuni e collettività è stato posto in luce da David Harvey in uno studio su Marx e i *commons*[89]. È illuminante come, portando Locke alle sue estreme conseguenze, si può affermare che il diritto di proprietà nasce collettivo e non privato. Semplificando la lettura prevalente di Locke, si può dire che gli individui sono titolari della proprietà sui frutti del proprio lavoro, da cui segue che quegli individui i quali non generano valore tramite il proprio lavoro non possono essere titolari di diritti dominicali[90]. Marx smaschera la finzione lockiana: poiché nella fabbrica il lavoro è organizzato su base collettiva, se dal lavoro fluiscono diritti di proprietà questi devono essere collettivi. Nell'IoT è chiaro che la principale merce prodotta e scambiata sui mercati *smart* è costituita dai dati[91]. Se si accetta questa premessa, ne segue a rigore che noi utenti di questi dispositivi, in quanto produttori di dati, non siamo dissimili dagli operai, con la differenza che non siamo consapevoli di esserlo e che il lavoro si estende al di fuori della fabbrica, per includere ogni luogo e ogni momento dell'esperienza terrena. La conclusione necessitata è che in quanto gli utenti 'smart' producono dati e quindi valore, su questi gli utenti-lavoratori inconsapevoli vantano diritti collettivi e le imprese IoT devono essere espropriate dei dati che a loro volta avevano sottratto agli utenti e, in ultima analisi, dei mezzi di produzione.

Questa collettivizzazione è legata doppio nodo col concetto di beni comuni, in particolare nella loro accezione di dominio della democrazia radicale[92], della cui fenomenologia variegata sono nota manifestazione le tante occupazioni e riappropriazioni che, in Italia, hanno restituito alla collettività teatri, ex cinema, e altri spazi in stato d'abbandono (Teatro Valle di Roma, Coppola di Catania, ecc.). Riflettendo sulla nozione di beni comuni esemplificata dalle occupazioni, si è convincentemente osservato che le stesse identificano una «fase di effervescenza sociale e rappresentano un laboratorio di sperimentazione del "comune" di un bene in cui l'accento cade […] sulla sua gestione prima ancora che sulla sua fruizione»[93]. Su questi beni comuni dalla portata più eversiva voglio concentrarmi perché maggiore è il loro potenziale per contrastare le pratiche estrattive del capitalismo, inclusa la sua variante *smart*. Meno esplorate delle summenzionate occupazioni, ma nello stesso solco, sono quelle esperienze e pratiche di

[87] DDL 1999 «Modifiche al codice civile in materia di classificazione e regime giuridico dei beni, nonché definizione della nozione di ambiente» (*DDL Rodotà*).
[88] Art. 812-bis, co. 1 c.c., come sarebbe stato inserito dal *DDL Rodotà*.
[89] Harvey 2017.
[90] Harvey 2011.
[91] V., *ex permultis*, Zheng *et al.* 2019.
[92] Bazzicalupo 2018.
[93] Nivarra 2016: 46.

resistenza collettiva benecomunista di matrice nera e queer[94]. Dal primo punto di vista, è emblematico che, dopo decenni di innovazioni normative che nulla avevano portato in termini di giustizia razziale, il vero giro di boa si è avuto quando collettività nere si sono organizzate nel movimento *black lives matter*. Il collegamento fra etnia e beni comuni appare con chiarezza a chi legga *The Sense of Brown*[95] di José Esteban Muñoz, dove lo studioso cubano-americano presenta il concetto di *brown commons*. Per comprenderlo bisogna far riferimento all'approccio di Muñoz ai concetti di razza ed etnia. Nel contribuire a una comprensione non ontologica e biologica di questi concetti – proponendo invece l'idea che l'etnia è costrutto storico e performativo – Muñoz suggerisce che razze ed etnia sono differenze affettive, cioè «ways in which different historically coherent groups "feel" differently and navigate the material world on a different emotional register»[96]. Questo 'sentire' non è una condizione individuale, piuttosto si tratta di un «larger collective mapping of self and other»[97]. Il concentrarsi sulla dimensione collettiva porta l'autore a presentare il concetto di *brown commons* non solo come un punto focale in cui l'etnia è 'sentita', ma anche – quel che più conta ai fini di questo saggio – come qualcosa che è «not about the production of the individual but instead about a movement, a flow, and an impulse, to move beyond the singular and individualized subjectivities»[98]. Ed è in questo movimento trascendente le individualità che si può trovare la spinta per resistere alle pratiche estrattive dei capitalisti *smart*.

Non è un caso che Muñoz sia anche uno dei maggiori esponenti della teoria *queer*, che ha contribuito in modo non sottovalutabile a smantellare le fondamenta del capitalismo[99]. In effetti, l'accezione radicale di beni comuni non può essere compresa a pieno se non riferendosi anche al *queer commons*. Come è stato evocativamente osservato, l'attivismo *queer* immagina, sperimenta e implementa «the improvisational infrastructures necessary for managing the unevenness of contemporary existence»[100]. Le intersezioni fra resistenza queer e beni comuni abbondano, ma probabilmente l'esempio più significativo è l'occupazione di Gezi Park in Turchia che, portando in piazza oltre tre milioni e mezzo di manifestanti, fu forse il momento più difficile per il regime di Erdoğan. Ciò che forse è meno noto è che Gezi Park era un luogo *queer* di *cruising* e prostituzione e che proprio collettivi di persone LGBTQ+ svolsero un ruolo importante nell'occupazione e nelle proteste[101].

Queste e altre forme di resistenza a tutela dei beni comuni si sono per lo più concentrate su risorse naturali, edifici e beni materiali, piuttosto che su beni immateriali come la conoscenza, l'Internet e i dati[102]. Ciò che vorrei brevemente esplorare è se sia possibile immaginare un futuro in cui saliremo sulle barricate non solo per riprenderci un teatro o un parco, ma anche per riprenderci l'internet.

---

[94] Sia nero che queer vengono qui intesi nella loro accezione politica di collettività di oppressi che rifiutano l'ortodossia di una società a, rispettivamente, bianchezza ed eterosessualità presunte e privilegiate.
[95] Muñoz: 2020.
[96] Muñoz: 2000: 70.
[97] Muñoz: 2013: 415.
[98] Muñoz: 2020: 397.
[99] In Italia, un ruolo simile fu svolto da Mieli 1977.
[100] Millner-Larsen, Butt 2018: 4.
[101] Özbay, Savcı 2018.
[102] Molte delle battaglie riguardanti beni materiali avevano il fine indiretto di tutelare beni immateriali ad es. quando volevano ridestinare a usi culturali edifici commerciali. Ciò su cui mi voglio concentrare è la resistenza che si indirizzi *recta via* ai beni immateriali e ai beni *smart*.

Anche considerata l'importanza del *queer commons*, mi pare abbia senso cominciare col c.d. *techlash* (crasi fra *technology* e *backlash*, la decisa reazione negativa di una collettività a cambiamenti o eventi sociali o politici)[103]. Il *techlash* è la reazione della società civile e dei legislatori a una serie di scandali – avente le sue scaturigini da Cambridge Analytica – da cui seguì un atteggiamento di sfiducia e sospetto nei confronti delle società *big tech*. L'analisi giuridica si è occupata per lo più di strumentalizzare il *techlash* per pretendere a gran voce la necessità di riforme che imbrigliassero queste multinazionali[104]. Più che concentrarmi sulla risposta normativa, mi pare particolarmente interessante, soprattutto in un paese e in un settore dove i sindacati sono stati ridotti a un ruolo quasi irrilevante[105], occuparmi della spontanea organizzazione dei lavoratori delle multinazionali *big tech* per reagire a decisioni commerciali considerate irresponsabili o immorali[106]. Il collegamento col *queer commons* si rinviene nella più nota esponente del più importante di questi episodi di resistenza. Mi riferisco a Rebecca Rivers, un'ingegnera informatica trans ai tempi impiegata da Google che fu licenziata poco dopo avere fatto *coming out*[107]. Rivers era a capo di una rivolta dei lavoratori contro Google quando il gigante della pubblicità prese la dubbia decisione di mettere a disposizione dell'US Department of Defense le proprie tecnologie IA per consentire alle forze armate statunitensi di identificare e tracciare persone e veicoli nei video registrati dai droni. Inorriditi dalla possibilità che le tecnologie a cui avevano contribuito potessero essere usate in guerra e notando lo scollamento dai principi etici a cui pure Google aveva dichiarato di aderire, i lavoratori si organizzarono (con petizioni, *town halls*, ecc.) e riuscirono a costringere la società a non rinnovare il contratto. Simili metodi furono utilizzati per bloccare altri progetti (ad es. Dragonfly)[108] e dai lavoratori di altre multinazionali *big tech*[109].

Mentre si può ipotizzare che almeno una delle ragioni di queste forme di resistenza collettiva fosse il risvolto materiale di queste ingiustizie immateriali – ad es. l'uso dell'IA per neutralizzare obiettivi militari – bisogna riconoscere che non si trattava di IoT in senso stretto. Con ciò non voglio dire che non sia possibile rinvenire esempi di resistenza nel dominio in esame. E l'esempio principe ci porta in Ucraina. Ho accennato *supra* al produttore di trattori *smart* che avevano privato i contadini americani del diritto di riparare i propri trattori, grazie a una combinazione di potere contrattuale, tecnologico e PI. Ho omesso di dire che la soluzione

[103] Holmberg 2022 si concerta su come questa reazione alla dominanza di *big tech* stia conducendo – financo nei liberisti Stati Uniti, tradizionalmente contrari a limitare la libertà d'impresa – all'approvazione di leggi atte a controllare il potere delle piattaforme (segnatamente l'*American Innovation and Choice Online Act* e l'*Open App Markets Act*).

[104] Sui limiti di questo approccio v. la convincente critica di Viljoen 2021b.

[105] In Europa, per converso, i sindacati stanno svolgendo un ruolo molto importante nel cambiare il corso dell'economia dei dati in un senso più equo. V. ad es. il caso dell'algoritmo Frank di Deliveroo Italia s.r.l. in Trib. Bologna, sez. lav., ord. 31 dicembre 2020, in *DRI*, 2021, 1, 204 con nota di Faioli 2021.

[106] Su, Lazar, Irani 2021.

[107] V., *amplius*, Conger, Scheiber 2020.

[108] Si trattava di un programma segreto per cui Google avrebbe censurato determinati risultati delle ricerche per conto del Governo cinese (Shaban 2018).

[109] (Teachout 2020). Attualmente, un contratto da cui sta scaturendo una rivolta (questa volta tanto degli impiegati quanto degli azionisti) è «*Project Nimbus*» in virtù del quale Amazon e Google porterebbero tutti i server del cloud del Governo israeliano all'interno del territorio israeliano e si impegnerebbero a mantenere la continuità del servizio. Ciò consentirebbe a detto Governo di essere immune alle pressioni politiche derivanti dall'occupazione della Palestina, che altrimenti potrebbero portare a boicottaggi a livello internazionale e sanzioni prendenti di mira il cloud pubblico israeliano. V. Biddle 2022.

non venne trovata – immediatamente e solo – in Parlamento[110]. Piuttosto, la soluzione si rinvenne nell'inaspettata collaborazione fra collettivi di hacker ucraini – che crearono una versione 'pirata' del software incorporato nei trattori John Deere – e i collettivi di agricoltori americani, che scaricarono e condivisero ampiamente il software per riappropriarsi del diritto di riparare i propri trattori. Questo movimento, che non è isolato (si pensi ad es. a *Farm Hack*)[111] dimostra almeno due cose. In primo luogo, che il potenziale antagonistico dei beni comuni si può esprimere nell'extragiuridico, financo nell'antigiuridico. Soltanto in questo senso, i beni comuni cessano di essere innocui e diventano incandescenti, in quanto «si propon[gono] di mettere in discussione l'assetto dominante nel suo insieme»[112]. In secondo luogo, che il conflitto ha già cominciato ad estendersi, non solo dal materiale all'immateriale, ma anche allo *smart*.

Se la portata eversiva di occupazioni e *hacking* è di più immediata evidenza, ritengo che vadano anche considerate tutte le forme di organizzazione fluida e dal basso in cui le collettività di riferimento riprendono il controllo sull'IoT[113]. Visti i limiti del presente contributo, questi non potranno che essere analizzati a volo d'uccello. Ad esempio, un ottimo studio sulle *smart cities* ha riportato una serie di «good examples of citizen-led movements to reclaim urban resources as common goods»[114], ad es. Il Piano Digitale di Barcellona avente come obiettivo la costruzione di un *data commons*. Come Morozov e Bria evidenziano, mediante alleanze progressive – fra città, movimenti e organizzazioni politiche – e tramite investimenti pubblici in infrastrutture per i dati aperti e sistemi di welfare orientati al bene comune è possibile passare «from surveillance capitalism to a system capable of socializing data and experimenting with new forms of cooperativism»[115].

Mentre sarebbe auspicabile che i corpi rappresentativi dello Stato e degli enti locali incentivassero la socializzazione dei dati e consimili misure benecomuniste, è anche vero che se vogliamo riprenderci il mondo 'smart' restare in attesa di interventi pubblici tradirebbe una visione ingenuamente irenica delle forze in gioco. Ad esempio, non si vede come si possa delegare il cambiamento nella governance delle tecnologie a riforme legislative quando è noto a tutti che le imprese *big tech*, include quelle dell'IoT, sono diventate esse stesse legislatrici o (i) tramite pratiche di *lobbying* incessanti e opache[116]; o (ii) mediante le regole private inscritte nel design delle tecnologie stesse, sempre più a ciò incentivate da interventi normativi che

[110] Mentre a livello statale e di pratica dell'US Copyright Office qualche progresso è stato fatto, il fronte federale a favore del *right to repair* stenta ancora ad affermarsi, anche se si segnala che a Luglio 2022, Joe Biden ha ordinato alla Federal Trade Commission e al Department of Agriculture to migliorare l'accesso a servizi di riparazione sia ai consumatori che agli agricoltori (*Executive Order on Promoting Competition in the American Economy*, July 9, 2022).

[111] Farm Hack è una comunità globale di agricoltori che costruiscono e modificano i propri attrezzi e li condividono sia online che in meet-up. Fra gli attrezzi e sistemi di più recente sviluppo si segnala FarmOS, un sistema F/LOSS per la gestione e la contabilità nelle imprese agrarie e fattorie. V. <https://farmhack.org/tools>.

[112] Nivarra 2016: 61.

[113] Nella quadripartizione proposta da Nivarra (2016) questa declinazione dei beni comuni probabilmente non andrebbe accorpata alle occupazioni, essendo in certa misura istituzionale. Almeno dalla prospettiva dell'IoT, i confini definitori mi paiono meno nitidi di quanto non si possa ritenere.

[114] Morozov, Bria 2018: 26.

[115] Morozov, Bria 2018: 53.

[116] Farrand 2015; Gan 2017.

delegano ai privati la regolazione tecnologica (ad es. l'*upload filter*)[117]. Se undici anni fa un gruppo di cittadini romani non avesse occupato l'Ex Cinema Palazzo per evitare che diventasse un casinò, oggi Roma Capitale non avrebbe avviato il processo per riportare l'edificio in mano pubblica[118]. L'IoT porta con sé la speranza che la stessa fattiva impazienza possa svilupparsi anche nei confronti dei beni immateriali e *smart*. Nell'era della rimaterializzazione, in cui materiale e immateriale si fondono per diventare *smart*, ci si può attendere che quello stesso rapporto viscerale che ci lega alle cose tangibili – cui è legata la potente forze evocativa del diritto di proprietà[119] – si sviluppi nei confronti dei beni *smart* e che da ciò alfin segua la spinta per salire sulle barricate e 'occupare' l'IoT.
La vicenda dei trattori hackerati potrebbe essere solo l'inizio. Nell'IoT iniziative dal basso e partecipative abbondano *inter alia* ad Arduino, TrustableTech, DotEveryone, Open, OpenTech UK e Arribada Restart Project. Si pensi all'enorme massa critica costituita dai 2000 meetup in giro per il mondo – molti nel Sud globale – con un milione e mezzo di cittadini impegnati a realizzare un IoT più giusto, inclusivo e al servizio delle collettività[120].

5. Inizi

I capitalisti smart pongono in essere una vasta gamma di pratiche estrattive, dall'espropriazione dei dati al controllo dei nostri dispositivi tramite un coacervo di poteri di matrice giuridica, tecnologica e fattuale. Ciò che a primo acchito può apparire come la morte della proprietà (sui nostri dispositivi), può essere meglio compresa come una tragedia degli «*smart anticommons*» consumata per mano di imprese IoT che monetizzano la nostra esistenza e trasformano l'internet nel teatro della terza *enclosure*.
Il diritto, plasmato direttamente o indirettamente dai padroni e sottomesso alle ragioni del libero mercato, è difficile possa fornire risposte soddisfacenti a questi problemi. I beni comuni, per converso, possono costituire una soluzione assai più efficace, nella duplice accezione di alfieri dell'*open source* e punti di emersione di pratiche di resistenza collettiva.
Quanto alla 'apertura', il riferimento più immediato è al F/LOSS, col caveat che occorre vada distinto dalla sua variante depoliticizzata (l'OSS) e che non si può riporre ogni speranza di trasparenza e affidabilità nel F/LOSS, senza tenere conto delle altre pratiche estrattive e ostruttive che consentono alle società dell'IoT di intorpidire le acque. Nell'IoT, è importante tenere a mente che – data la natura ibrida dei beni *smart*, amalgama di hardware, software, servizi, contenuti digitali e dati – occorre aprire ogni componente, non solo il sorgente del software incorporato nel dispositivo *smart*. In questo saggio mi sono incontrato sull'apertura dell'hardware, delle piattaforme e dei dati. Gli ostacoli giuridici, politici e tecnici a quest'apertura olistica abbondano, ma su ognuno di questi piani è possibile individuare soluzioni. Dopo quasi un decennio trascorso a studiare il capitalismo *smart*, mi sono convinto

[117] Il riferimento è alle nozioni – sovrapponibili nel loro nocciolo semantico – di «code as law» (Lessig 2006), «regulation by design» (Urquhart, Rodden 2016), «technological management» (Brownsword 2019) e «algorithmic regulation» (Yeung, Lodge 2019).
[118] *Ex Cinema Palazzo: Campidoglio, chiesta a proprietà manifestazione di interesse a cedere stabile*, 2021.
[119] Ad es., alle origini del *droit d'auteur* vi è la battaglia fra i librai parigini e quelli della provincia e, sorprendentemente, il dispositivo retorico a cui entrambe le fazioni si affidarono fu proprio quello della proprietà Moscati 2007: 270 e passim.
[120] *Internet of Things groups*, 2022.

che la principale risposta possa essere fornita dal basso, da collettività che si organizzano in modi più o meno informali per resistere agli abusi dei capitalisti *smart*. La collaborazione fra gli hacker ucraini e gli agricoltori americani per riprendersi il diritto di riparare i propri trattori *smart* mi pare indichi la via da percorrere affinché noi cittadini possiamo diventare consapevoli che, siccome produciamo il valore chiave dell'IoT nella misura in cui produciamo dati, vantiamo diritti collettivi sugli stessi e l'unico modo per reclamarli è occupare l'IoT.

Bibliografia

Aliprandi, S. (ed.) (2014) *Il fenomeno open data: indicazioni e norme per un mondo di dati aperti*. Milano, Ledizioni.

Angiolini, C. (2020) *Lo statuto dei dati personali: uno studio a partire dalla nozione di bene*. Torino, Giappichelli.

Barker, K. *et al.* (2021) *Written evidence submitted by the British and Irish Law, Education and Technology Association (BILETA) (OSB0073)*. UK Parliament. Available at: https://committees.parliament.uk/writtenevidence/39201/html/.

Bazzicalupo, L. (2018) *Le diverse anime della democrazia radicale*, «Quadranti», VI(2), 56.

Benkler, Y. (1999) *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, «NYU Law Review», 74(2), 354.

Biddle, S.B. (2022) *Google and Amazon Face Shareholder Revolt Over Israeli Defense Work*, *The Intercept*. Available at: https://theintercept.com/2022/05/18/google-amazon-israel-military-nimbus/ (Accessed: 9 June 2022).

Big Data for Sustainable Development (2020) *United Nations*. United Nations. Available at: https://www.un.org/en/global-issues/big-data-for-sustainable-development (Accessed: 31 May 2022).

Borghi, M. (2018) *Portabilità dei dati e regolazione dei mercati digitali*, «Mercato Concorrenza Regole*»,* (2), 223–247. Available at: https://doi.org/10.1434/91151.

Boyle, J. (2010) *The Public Domain: Enclosing the Commons of the Mind*. Yale University Press.

Brownsword, R. (2019) *Law, technology and society: re-imagining the regulatory environment*. Abingdon, Oxon; New York, NY, Routledge (Law science and society).

Caso, R. (2022) *Open Data, ricerca scientifica e privatizzazione della conoscenza*. Trento LawTech Research paper nr. 48. Available at: https://doi.org/10.5281/zenodo.5902766.

Caterina, R. (2010) *Il possesso*, in *Trattato dei diritti reali. Vol. 1 Proprietà e possesso*. Giuffrè.

Cohen, J.E. (2019) *Between truth and power: the legal constructions of informational capitalism*. New York, NY, Oxford University Press.

Conger, K. and Scheiber, N. (2020) *The Great Google Revol*t, «New York Times Magazine». Available at https://www.nytimes.com/interactive/2020/02/18/magazine/google-revolt.html (Accessed 1 August 2022).

Elvy, S.-A. (2021) *A commercial law of privacy and security for the internet of things*. Cambridge, United Kingdom; New York, NY, Cambridge University Press.

Estèves, N. (2018) *Open models for patents: Giving patents a new lease on life?*, «The Journal of World Intellectual Property», 21(1–2), 2–14. Available at: https://doi.org/10.1111/jwip.12089.

Ex Cinema Palazzo: Campidoglio, chiesta a proprietà manifestazione di interesse a cedere stabile (2021) *Roma Capitale*. Available at: https://www.comune.roma.it/web/it/notizia.page?contentId=NWS763115 (Accessed: 10 June 2022).

Faioli, M. (2021) *Discriminazioni digitali e tutela giudiziaria su iniziativa delle organizzazioni sindacali*, «Diritto delle Relaazioni Industriali», (1), 204.

Fairfield, J.A. (2017) *Owned: Property, privacy, and the new digital serfdom*. Cambridge University Press.

Farrand, B. (2015) *Lobbying and Lawmaking in the European Union: The Development of Copyright Law and the Rejection of the Anti-Counterfeiting Trade Agreemen*t, «Oxford Journal of Legal Studies», 35(3),487–514. Available at: https://doi.org/10.1093/ojls/gqu028.

Fia, T. (2021) *An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons*, «Global Jurist», 21(1), 181–210. Available at: https://doi.org/10.1515/gj-2020-0034.

Floridi, L. (2020) *Pensare l'infosfera. La filosofia come design concettuale*. Cortina Raffaello.

Frosio, G. and Bulayenko, O. (2021) *Website Blocking Injunctions in Flux: Static, Dynamic, and Live*, «Journal of Intellectual Property Law & Practice», 16(3), 1127.

Frosio, G.F. (2017) *The Death of "No Monitoring Obligations": A Story of Untameable Monsters*, «Journal of Intellectual Property, Information Technology and Electronic Commerce Law», 8(3). Available at: http://www.jipitec.eu/issues/jipitec-8-3-2017/4621.

Gan, H.Z. (2017) *Corporations: The Regulated or the Regulators-The Role of IT Companies in Tackling Online Hate Speech in the* EU, «Columbia Journal of European Law», 24, 111.

Geiger, C. and Jütte, B.J. (2022) *The future of content moderation in the EU after the Court of Justice's ruling upholding the validity of Article 17 CDSM Directive (Case C-401/19)*, *EU Law Live*. Available at: https://eulawlive.com/op-ed-the-future-of-content-moderation-in-the-eu-after-the-court-of-justices-ruling-upholding-the-validity-of-article-17-cdsm-directive-case-c-401-19-by-christophe-geiger/ (Accessed: 3 June 2022).

Ghosh, S. (2007) *How to build a commons: Is intellectual property constrictive, facilitating, or irrelevant?*, in C. Hess and E. Ostrom (eds) *Understanding knowledge as a commons: From theory to practice*. MIT Press, 209.

Glick, B. (2016) *Executive interview: Harriet Green, IBM's internet of things chief*, *Computer Weekly*. Available at: http://www.computerweekly.com/news/450280673/Executive-interview- Harriet-Green-IBMs-internet-of-things-chief.

Google Open Source (2022). Available at: https://opensource.google/ (Accessed: 3 June 2022).

Grossi, P. (1977) *Un altro modo di possedere. L'emersione di forme alternative di proprietà alla coscienza giuridica postunitaria*. Giuffrè.

Grossi, P. (2007) "*Un altro modo di possedere" rivisitato*, «Agricoltura Istituzioni Mercati», (1), 11.

Guochao, Z. *et al.* (2021) *Digital music copyright management system based on blockchain*, «Journal of Computer Applications», 41(4), 945.

Hardin, G. (1968) *The tragedy of the commons: the population problem has no technical solution; it requires a fundamental extension in morality*, «Science», 162(3859), 1243–1248.

Hardt, M. and Negri, A. (2009) *Commonwealth*. Cambridge, Mass., Harvard University Press.

Harvey, D. (2011) *The Future of the Commons*, «Radical History Review», 2011(109), 101–107. Available at: https://doi.org/10.1215/01636545-2010-017.

Harvey, D. (2017) *Marx, Capital and the madness of economic reason*. London, Profile.

Heller, M. (2013) *The tragedy of the anticommons: A concise introduction and lexicon*, «Modern Law Review», 76(1), 6–25.

Hess, C. and Ostrom, E. (eds) (2007) *Understanding Knowledge as a Commons. From Theory to Practice*. MIT Press.

Hilty, R. *et al.* (2021) *Covid-19 and the role of intellectual property: position statement of the Max Planck Institute for innovation and competition of 7 May 2021*, «Max Planck Institute for Innovation & Competition Research Paper» [Preprint], (21–13). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841549 (Accessed 1 August 2022).

Holmberg, S. (2022) *The techlash is the first step to restoring a fair US economy*, «Financial Times», 15 February 2022.

IBM Closes Landmark Acquisition of Red Hat for $34 Billion; Defines Open, Hybrid Cloud Future (2019) *Red Hat*. Available at: https://www.redhat.com/en/about/press-releases/ibm-closes-landmark-acquisition-red-hat-34-billion-defines-open-hybrid-cloud-future (Accessed: 3 June 2022).

Internet of Things groups (2022) *Meetup*. Available at: https://www.meetup.com/topics/internet-of-things/ (Accessed: 10 June 2022).

Jan, R. *et al.* (2018) *The European Tracking Network: Connecting biotelemetry users in Europe*, in Mees, J. et al. (ed.) *Book of abstracts – 53rd European Marine Biology Symposium*, Oostende, Belgium, 17-21 September 2018. VLIZ Special Publication. Vlaams Instituut voor de Zee, 87.

Kang, H.Y. *et al.* (2021) *Academic Open Letter in Support of the TRIPS Intellectual Property Waiver Proposal*. SSRN Scholarly Paper 3885568. Rochester, NY, Social Science Research Network. Available at: https://doi.org/10.2139/ssrn.3885568.

Karmel, B. (2020) *Content portability in the EU: challenges and pragmatic solutions*, «European Intellectual Property Review», 42(7), 414–425.

Lessig, L. (2006) *Code*. *Version 2.0.* New York, Basic Books.

Lloyd, W.F. (1980) *WF Lloyd on the Checks to Population*, «Population and Development Review», 6(3), 473–496.

Maggiolino, M. and Montagnani, M.L. (2011) *From Open Source Software to Open Patenting − What's New in the Real of Openness?*, «International Review of Intellectual Property and Competition Law», 42(7), 804.

Meta Open Source (2022). Available at: https://opensource.fb.com/ (Accessed: 3 June 2022).

Michels, J.D. and Millard, C. (2022) *The New Things: Property Rights in Digital Files?*, «The Cambridge Law Journal», 1–33. Available at: https://doi.org/10.1017/S0008197322000228.

Microsoft Open Source (2022) *Microsoft Open Source*. Available at: https://opensource.microsoft.com/ (Accessed: 3 June 2022).

Mieli, M. (1977) *Elementi di critica omosessuale*. Einaudi.

Millner-Larsen, N. and Butt, G. (2018) *Introduction*, «GLQ: A Journal of Lesbian and Gay Studies», 24(4), 399–419. Available at: https://doi.org/10.1215/10642684-6957744.

Montagnani, M.L. (2019) *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, «Mercato Concorrenza Regole», (2), 293–314. Available at: https://doi.org/10.1434/95581.

Monterossi, M.W. (2020) *Estrazione e (ri)utilizzo di informazioni digitali all'interno della rete internet. Il fenomeno del c.d. web scraping*, «Diritto dell'informazione e dell'informatica», II(2), p. 327. NOME COMPLETO RIVISTA

Morozov, E. and Bria, F. (2018) *Rethinking the smart city. Democritizing urban technology*. Rosa Luxemburg Stiftung New York Office. Available at: http://www.rosalux-nyc.org/rethinking-the-smart-city/ (Accessed: 17 November 2020).

Moscati, L. (2007) *Alle radici del Droit d'auteur*. Monduzzi Editore.

Muñoz, J.E. (2000) *Feeling Brown: Ethnicity and Affect in Ricardo Bracho's The Sweetest Hangover (and Other STDs)*, «Theatre Journal», 52(1), 67–79. Available at: https://doi.org/10.1353/tj.2000.0020.

Muñoz, J.E. (2013) *Feeling Brown, Feeling Down: Latina Affect, the Performativity of Race, and the Depressive Position*, in D.E. Hall and A. Jagose (eds) *The Routledge Queer Studies Reader*. Routledge, 412.

Muñoz, J.E. (2020) *The sense of brown*. Edited by T.A. Ochieng' Nyongó and J.T. Chambers-Letson. Durham, Duke University Press (Perverse modernities).

Nivarra, L. (2007) *Il diritto d'autore*, in C. Castronovo and S. Mazzamuto (eds) *Manuale di diritto privato europeo*. Giuffrè, 497.

Nivarra, L. (2016) *Quattro usi di "beni comuni" per una buona discussione*, «Rivista critica di diritto privato», 1, 43.

Noto La Diega, G. (2022) *Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies*. Routledge.

Noto La Diega, G. and Derclaye, E. (forthcoming) *Opening Up Big Data for Sustainability: What Role for Database Rights in the Fourth Industrial Revolution?*, in O.-A. Rognstad, T. Pihlajarinne, and J. Mähönen (eds) *Promoting Sustainable Innovation and the Circular Economy: Legal and Economic Aspects*. Routledge.

Noto La Diega, G. and Sappa, C. (2020) *The Internet of Things at the intersection of data protection and trade secrets. Non-conventional paths to counter data appropriation and empower consumers*, «Revue européenne de droit de la consommation», (3), 419.

Noto La Diega, G. and Stacey, J. (2018) *Can Permissionless Blockchains be Regulated and Resolve Some of the Problems of Copyright Law?*, in Ragnedda, M. and Destefanis, G. (eds) *Blockchain and Web 3.0*. Social, Economic, and Technological Challenges. Routledge,30.

Noto La Diega, G. and Walden, I. (2016) *Contracting for the "Internet of Things": looking into the Nest*, «European Journal of Law and Technology», 7(2). Available at: http://ejlt.org/article/view/450 (Accessed: 30 April 2019).

Open Invention Network (OIN) (2022) *Open Invention Network*. Available at: https://openinventionnetwork.com/ (Accessed: 3 June 2022). AUTORE, IF ANY?

Özbay, C. and Savcı, E. (2018) *Queering Commons in Turke*y, «GLQ: A Journal of Lesbian and Gay Studies», 24(4), 516–521. Available at: https://doi.org/10.1215/10642684-6957870.

Palmirani, M. *et al.* (2018) *Le licenze per il rilascio degli Open Data della Pubblica Amministrazione. Prime riflessioni alla luce dalla Direttiva UE 2019/1024*, «Diritto Mercato Tecnologia» [Preprint]. Available at: https://www.dimt.it/la-rivista/articoli/licenze-rilascio-open-data-pa/ (Accessed: 7 June 2022).

Pasquale, F. (2015) *The Black Box Society*. Harvard University Press.

Perel, M. and Elkin-Koren, N. (2017) *Black box tinkering: Beyond disclosure in algorithmic enforcement*, «Florida Law Review»., 69, 181.

Ponciano, J. (2022) *The World's Largest Tech Companies In 2022: Apple Still Dominates As Brutal Market Selloff Wipes Trillions In Market Value*, *Forbes*. Available at: https://www.forbes.com/sites/jonathanponciano/2022/05/12/the-worlds-largest-technology-companies-in-2022-apple-still-dominates-as-brutal-market-selloff-wipes-trillions-in-market-value/ (Accessed: 3 June 2022).

della Ratta, F. *et al.* (2018) *Twitter e la statistica ufficiale: il dibattito sul mercato del lavoro* Proceedings of the 14th International Conference on Statistical Analysis of Textual Data. UniversItalia, 200.

Sappa, C. (2021) *Access and re-use of public sector information in a copyright perspective*, in I. Stamatoudi and P. Torremans (eds) *EU Copyright Law*. Edward Elgar Publishing, 762–781. Available at: https://doi.org/10.4337/9781786437808.00028.

Savelyev, A. (2014) *Software-as-a-service–Legal nature: Shifting the existing paradigm of copyright law*, «Computer Law & Security Review», 30(5), 560–568.

Scandola, S. (2021) *Recesso e responsabilità del gestore di un social network in caso di disattivazione ingiustificata del profilo di un utente*, «GiustiziaCivile.com», 8, X, 1.

Shaban, H. (2018) *Google employees go public to protest China search engine Dragonfly*, «The Washington Post». Available at https://www.washingtonpost.com/technology/2018/11/27/google-employees-go-public-protest-china-search-engine-dragonfly/ (Accessed on 1 August 2022).

Stallman, R. (2022) *Why Open Source Misses the Point of Free Software*, *GNU Project*. Available at: https://www.gnu.org/philosophy/open-source-misses-the-point.html (Accessed: 2 June 2022).

Su, N.M., Lazar, A. and Irani, L. (2021) *Critical Affects: Tech Work Emotions Amidst the Techlash*, *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1), 1–27.

Teachout, Z. (2020) *Break'em up: Recovering our freedom from big ag, big tech, and big money*. All Points Books.

Temmerman, L. and Van den Broeck, W. (2021) *The Decolonisation of the Smart City through Degrowth and Serendipity*, in. *2021 IEEE International Smart Cities Conference (ISC2)*, IEEE, 1–4.

Tennison, J. (2020) *Individual, collective and community interests in data*, «Jeni's Musings», 27 December. Available at: http://www.jenitennison.com/2020/12/27/individual-collective-community.html (Accessed: 27 July 2021).

Urquhart, L. and Rodden, T. (2016) *A Legal Turn in Human Computer Interaction? Towards "Regulation by Design" for the Internet of Things*, «SSRN Electronic Journal» [Preprint]. Available at: https://doi.org/10.2139/ssrn.2746467.

Viljoen, S. (2021a) *Democratic Data: A Relational Theory For Data Governance*, «Yale Law Journal», (2), 573. Available at: https://doi.org/10.2139/ssrn.3727562.

Viljoen, S. (2021b) *The Promise and Limits of Lawfulness: Inequality, Law, and the Techlash*, «Journal of Social Computing», 2(3), 284–296. Available at: https://doi.org/10.23919/JSC.2021.0025.

Wark, M. (2021) *Capital Is Dead: Is This Something Worse?* Verso Books.

Wen, S.-F., Kianpour, M. and Kowalski, S. (2019) *An empirical study of security culture in open source software communities*, in *Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. *ASONAM '19: International Conference on Advances in Social Networks Analysis and Mining*, Vancouver British Columbia Canada: ACM, pp. 863–870. Available at: https://doi.org/10.1145/3341161.3343520.

Westkamp, G. (2010) *Code, Copying, Competition: The Subversive Force of Para-Copyright and the Need for an Unfair Competition Based Reassessment of DRM Laws after Infopaq*, «Journal of the Copyright Society of the USA», 58, 665.

Who owns the personal data you collect from users? (2020) «GetTerms.io», 6 February. Available at: https://getterms.io/blog/who-owns-the-personal-data-you-collect-from-users/ (Accessed: 8 June 2022).

Winner, L. (1980) *Do Artifacts Have Politics?*, «Daedalus», 109(1), 121–136.

Yeung, K. and Lodge, M. (eds) (2019) *Algorithmic regulation*. New York, NY, Oxford University Press.

Zheng, Z. *et al.* (2019) *Challenges and opportunities in IoT data markets*, in. *Proceedings of the fourth international workshop on social sensing*, ACM, 1–2.

Zuboff, S. (2019) *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. First edition. New York, PublicAffairs.