

Digital Authoritarianism

Brian Gannon

Fachgruppe IT und Technik
IU Internationale Hochschule,
Erfurt, Germany
e-mail: brian.gannon@iu.org

Abstract— Modern democratic societies have in recent centuries adopted a social contract whereby deference is shown by citizens, to state or public authority (and to the laws and institutions through which that authority is expressed) in return for a voice that determines the nature and extent of that authority. This social contract is now threatened by the emergence of a small number of private organizations which have assumed some of the functions of state authority. This shift from public to private authority has been enabled by the extent to which these private organizations – very large online platforms – use powerful tools to exploit vast amounts of data amassed over the past few decades. It has profound implications for individuals, particularly in respect of their fundamental human rights, and it undermines the basis of the contract that binds citizen and state. This gradual expansion of private digital power at the expense of public authority, described here as digital authoritarianism, is the subject of this research.

Keywords- *digital sovereignty; authoritarianism; online surveillance.*

I. INTRODUCTION

Digital platforms have developed highly lucrative and successful business models which are predicated on the fact that their raw material – personal data – is provided willingly and for free by individual users in exchange for access to online services provided by the digital platforms. They have taken advantage of rapid advances in technology, widespread connectivity, and associated network effects to establish dominant positions in the online marketplace. This condition is greatly enhanced by the conjunction of ubiquitous intelligent devices (the ‘Internet of Things’ – ‘IoT’) and powerful Artificial Intelligence (AI) technology.

From this vantage point, digital platforms have induced in users a profound deference to digital authority, engendered primarily by a demand for convenience. While the economic and normative effects of digital authoritarianism are eloquently described by Cohen, Pasquale, Zuboff and others, this paper focuses on describing the dependence/deference duality and its intersection with convenience [10][36][49]. The entrenchment of digital authority is diminishing human agency and thus has significant implications for society, its governing institutions and the rule of law.

The research is exploratory. It assesses the operation of digital platforms in enabling control and surveillance, recognizing that platforms have other powerful capabilities

and effects, alluded to but not investigated. It starts by setting out contextual underpinning for the analysis in Section 2; describing the types of enabling infrastructure that will transform its current capability in Section 3; and elaborating on the entrenchment of the digital authoritarian construct as an inevitable outcome of these developments in Section 4. Section 5 summarizes the role of regulation in constraining the digital authoritarian environment, and Section 6 presents a conclusion and future work.

II. CONTEXT: ANTECEDENTS, DEFINITIONS, FOUNDATIONS

A. Summary of literature and definitions

The most relevant antecedents for this discussion in the context of wider academic research are the notions of digital sovereignty, and of control and choice in cyberspace. The analysis starts by defining key terms.

‘Digital platform’ is used here as an umbrella term to describe private companies that provide large-scale digital infrastructure and services including search, social media, cloud computing, e-commerce, and operating systems to billions of users worldwide. It covers various aspects of these firms, including both technical capability and their business models. The digital platform is highly visible in a way that computing rarely was in the past. It is an entrenched social construct as much as a technical phenomenon, infecting language, custom, behavior, norms and even personal relationships. It not only facilitates human expression and interaction but also molds it, shaping opinion, generating ideas, entertaining, unearthing and disseminating knowledge, enabling commerce, and aiding destruction. It is nonetheless a new phenomenon, and its effects are incompletely understood.

‘Authoritarianism’ is usually understood in political terms and often used synonymously with the term ‘totalitarian’. Diebert defines authoritarianism as ‘...state constraints on legitimate democratic political participation, rule by emotion and fear, repression of civil society, and the concentration of executive power in the hands of an unaccountable elite.’ [14]. By extension, in this research ‘digital authoritarianism’ defines a state of society where important aspects of a citizen’s life are determined by data

gathered by ubiquitous sensors and analyzed to provide real-time regulation, recommendation and guidance. In such circumstances, the data (or the party holding the data) is the authority and the citizen is authorized to act according to the data. In the context of the online world an essential element of authoritarianism is the concentration of power in the hands of a few unaccountable individuals.

‘AI’ is described as adaptive computer activity that ‘arises when computer systems perform more complex tasks which previously required human intelligence ...<involving> machines which are capable of analyzing situations and learning for themselves and then generating answers which may not even be foreseen or controlled by their programmers.’ [38]. The distinguishing factor, emphasized in this definition, is foresight: traditional computing is eminently predictable - a computer does exactly what it is programmed to do, no more and no less, while AI systems may not. The deliberate ‘training’ of AI systems enhances their ability to predict and perform tasks. This is machine learning (ML), which seeks to mimic biological thought and learning processes [40].

The IoT is ‘an infrastructure in which billions of sensors embedded in common, everyday devices ... record, process, store and transfer data and... interact with other devices or systems’ [2]. IoT devices are often capable of actuation - taking action to adjust physical processes such as modifying temperatures. Hildebrandt conflates IoT with AI to define ‘data-driven’ agents - an ‘ambient intelligence’ that forms a ‘cyber-physical infrastructure’ which puts physical infrastructure such as homes, vehicles, fields, bio-forms and weapons online, ‘to enable persistent monitoring and surreptitious adaptation.’ [23]. In this research, the term ‘intelligent agent’ is used in a similar manner as a shorthand to cover the co-existence of IoT and AI capabilities in such agents.

B. *Digital Sovereignty*

The meaning of the term ‘digital sovereignty’ has changed over time, although the central concern – who controls and regulates the online environment – remains the same. Initially focused on regulation of cyberspace, subsequent inquiry addressed misuse of digital technology by state actors. For example, Diebert was predominantly concerned with risks of state authoritarianism through use of digital technology [14]. As the reach and scope of digital platforms grew, researchers explored the transfer of authority from state to private actors, described by Pasquale as ‘functional sovereignty’ [35]. In 2020, the chairman of the US House Judiciary Subcommittee on Antitrust, Commercial and Administrative Law questioned the heads of Amazon, Apple, Google and Facebook, noting that his committee’s investigation ‘...goes to the heart of whether we, as a people, govern ourselves, or whether we let ourselves be governed by private monopolies.’ [5].

Floridi defines sovereignty as a ‘...a form of legitimate, controlling power’, noting that until recently, it had always

been ‘analogue’, that is, bounded by the physical world (territories, cities, nations...), and controlling physical limited resources (land, oil, gold...) [19]. In the digital age, the infosphere is not a territory and ‘...digital assets are largely private and subject to market forces ...’ and ‘...whoever will win the fight for digital sovereignty will determine the lives of all people on both sides of the digital divide.’ [19].

Contemporary digital sovereignty is understood as an attempt by the state to reassert control over digital assets and information, so that the power of digital platforms to dictate terms is diminished. It implicitly acknowledges the incursions made by digital platforms into state domains and seeks to reverse these. The EU has led the way by laying the foundations of what Bradford describes as a ‘digital constitution’, meaning ‘...a set of expansive digital regulations that form a normative and principled foundation for a digital economy and society as construed by European laws.’ [4].

Regardless of the form of state governance adopted in the past, authority has invariably been public and, usually, visible: a citizen (or subject) might not always have been familiar with prevailing rules, actors, and institutions but generally knew who was in charge. In democratic societies, the citizen has scope to exercise her own judgement and to conduct her life within agreed legal boundaries. Fundamental rights are guaranteed according to the jurisdiction and these, along with social, economic and other rights (and associated obligations and constraints) afford a greater or lesser degree of *choice*. Similarly, the citizen as consumer may cede authority to private agents to effect control.

C. *Control, choice, consent, convenience*

The most frequent basis for engagement between user and digital platform is underpinned by the contractual notion of consent, effected through ‘opt-in’ or ‘opt-out’ choices. Thus, the individual consents to terms and conditions usually involving the surrender of personal data and receives software-based benefits such as social media apps for this consideration. Sometimes, consent is nugatory - the choice is ‘take it or leave it’.

This ‘informed consent’ mechanism is flawed, if not absolutely ‘...broken beyond any regulatory repair.’ [37]. This is because first, there is a cognitive deficit - the user is rarely fully informed of the nature and scope of her obligations, even if they are documented in the platform’s terms and conditions. Second, there is a structural deficit - the user can have little awareness of the wider use of her data when she consents to its collection. Third, there is an asymmetry between the trading partners that is heavily weighted in favor of the platform. A confounding factor is that many IoT devices eliminate the interface between user and data, making it difficult to collect consent.

The tension between control and choice or consent in the online environment is thus relevant. In the early days of the internet there was relative equality of arms between user and

provider, but now that digital platforms are weaponized with AI, IoT and other powerful controlling technology, user choice ‘...will inevitably be influenced by default rules, framing effects, and starting points’. [42]. Yeung identifies the inherent power of such choice architectures in influencing user behavior, that facilitate ‘undermining an individual’s capacity to exercise independent discretion and judgment’. [47]. Macro-economic and societal studies include Cohen’s comprehensive picture of the imbalance between corporate and individual actors online, and how this has unfolded and become entrenched; Pasquale’s extensive analysis of ‘black box’ algorithmic processes that deny choice; and, Zuboff’s forcible identification of online economic and social inequality as ‘surveillance capitalism’. [10][36][49].

A further overarching reason is convenience. Koops, discussing the role of consent in the context of data protection notes that, ‘(A)nother challenge of relying on consent is that convenience and people’s limited capacity to make rational decisions prevent people from seriously spending time and intellectual effort on reading the privacy statements of every website, app, or service they use.’ [28]. The demand for convenience in the digital environment is as persistent as it is offline. Consumers seek instant gratification, and digital platforms oblige with easy to use, intuitive interfaces offering simple ‘click here’ options, backed by impenetrable, formalistic contracts that are inconvenient to read. Digital platforms take advantage of consumer bias towards convenience and of their propensity to stick with default options, and use this propensity to influence and manipulate user choice [39][41]. The exacerbating effects on control and choice resulting from the widespread deployment of AI/ML technology by digital platforms are analyzed next.

III. EXPANSION OF DIGITAL PLATFORM CAPABILITY

A. Changes in digital platform capability

For the most part, citizens appear unconcerned by the coincidence of powerful new control and surveillance technologies in the hands of a few outside corporations. The services provided by digital platforms are often free, easy to use and have engendered social good. It is plausible to make a case that the benefit of such services, even if provided by a powerful oligopoly, outweigh potential risks.

The counterargument to complacency starts by highlighting the pace and scale of industrialization of surveillance, and the potential for almost unlimited control enabled by three directional trends. These are the *collection vector*: ubiquitous intelligent agents will generate vast real-time data sets; the *analysis vector*: powerful AI/ML technology will turbocharge efficient search, interrogation and manipulation of this data, generating actionable information; and the *distribution vector*: fast global networks will enable platforms to distribute the resulting information more efficiently than ever before. Together, this leads to greater dependence on, and deference to, digital platforms, and to a corresponding diminishment in human agency.

B. Collection, Analysis and Distribution

Notwithstanding the vast scale of data already compiled by digital platforms, and their ability to manipulate it, much data is incomplete and of poor quality. For example, in the UK’s National Health Service (NHS), many patient records are still paper-based [32]. The deployment of intelligent agents allows collection of data that is real-time, accurate, and independent of human agency. Conservative estimates suggest that more than 30 billion individual connected devices are already in place, and that annual growth rates of greater than 10% are predicted leading to deployment of hundreds of billions of devices by 2030 [13][26].

As with collection, analysis of data in the past has often been slow, cumbersome, and inaccurate. Now, availability of low-cost, high-performance processing and increased sophistication of analysis techniques mean that digital platforms are increasingly capable of accurate inference.

Together, the widespread deployment of connected smart devices combined with the deployment of advanced AI and ML capability trained on vast rich datasets extends the power and influence of digital platforms. This is because in addition to controlling the means of production of real-time, actionable, accurate information, they also control distribution.

At an infrastructural level, distribution capability is enhanced by 5G networks and almost total ubiquity of smart mobile handsets. This amplifies the power and effect of digital platforms across all spheres of social, commercial and political activity, including distribution of social mores and fashions via recommender and influencer functions, distribution and control of speech by controlling access to news platforms, and distribution of influence over democratic processes by targeting voters.

C. Emerging Effects of Intelligent Agents

Humans are willing to cede agency in this new technology landscape because it is increasingly convenient and easy. There is a view that it will in any case soon be impossible for users to exercise any meaningful agency. Yeung refers to Harari’s concept of ‘dataism’, a perception that the job of processing data into information should be left to intelligent algorithms because the human brain no longer has the capacity to process such vast amounts of data [48]. This operates in tandem with Morozov’s solutionism – the belief that technology can fix any problem. Intelligent agents ‘offer speed, lower transaction costs and efficiency in decision-making [21].

These viewpoints are evidence of an increasing reliance and deference to digital platforms. This amounts to a delegation of responsibility to unaccountable actors, and implies a more controlled and compliant society. This default to the ‘convenience’ option, and deference to the digital authorities who control the levers of information production, leads directly to digital authoritarianism.

IV. DIGITAL AUTHORITARIANISM

A. *Digital authoritarianism*

The conduct, ubiquity and reach of digital platforms has been described as ‘totalitarian’ by sources as ideologically opposed as Cuban communists and American capitalists [22][25]. The idea of extreme surveillance and control is not new: writing in 1787, Jeremy Bentham described the Panopticon and presented his Inspection Principle, paraphrased as ‘the more strictly we are watched, the better we behave’[3]. Foucault examined a similar theme in his writing on prisons [20]. More frequently, it is Orwell’s ‘Big Brother’ which provides the modern metaphor for Big Tech’s all-seeing eye [34]. In such descriptions, the emphasis is on total, comprehensive and always-on surveillance and control.

For digital platforms, totalitarianism is essentially a capitalistic process. Zuboff lays bare the economic rationale and ruthlessness underpinning the digital platform business model [49]. Her analysis implies that users view these platforms as *authorities*. It is certainly true that they are authoritative on social practice, style, rumor, commerce and much more. As digital platform knowledge is enhanced by information provided and analyzed by intelligent agents, the platform’s authority is correspondingly enhanced to the point where it leads to a state of ‘digital authoritarianism’.

Like Arendt’s totalitarianism, digital authoritarianism is: ‘... international in organization, all-comprehensive in its ...scope, and global in its ... aspiration...’ [1]. Unlike totalitarianism, the regime is not state imposed, nor does it incorporate tools of terror or extreme coercion. It is not politically inspired but commercial in intent: authority is vested not in the state or in elected officials but in private commercial agents. The nature of the social contract is one where the regime is sustained primarily by data volunteered by users in return for benefits and convenience (better health, safety, education, entertainment...) - a regime of bread and circuses rather than Big Brother.

B. *Normative implications of digital authoritarianism*

Arendt uses words such as ‘indifferent’, ‘apathetic’, ‘childish stupidity’, and ‘isolation’ to describe the readiness of the masses to accept totalitarian rule, embodying a form of deference that is not class or ideology-based, but is dependent on ‘the atomized and individualized mass’. [1]. While such attributes certainly assist in the establishment of a state of digital authoritarianism, the essential pre-condition is a demand for *convenience*.

This is not on its own a problem: services provided by digital platforms are easy to use, helpful and sometimes, wonderful. They operate as a public good, and like utilities have become indispensable. Search engines tell us what we know; online retailers tell us what we want; social media networks tell us who we are [15].

Yet, in providing convenience, digital services exacerbate the tyranny of choice [42]. The anxiety induced by choice is

relieved by authoritative decision-makers in the form of digital assistants (Alexa, Siri...), recommenders (GoCompare, Trip Adviser...), bots (autofill, chatbots...), and more. These are increasingly informed by distributed intelligent agents collecting data points and measurements that enhance the accuracy and relevance of the choice presented. AI-based inference lends further authority to digital platforms because of its predictive capability and ‘wisdom’.

This authority is at the heart of automation bias - the propensity for humans to defer to automated decision-making systems despite the presence of contradictory information. Errors of automation bias tend to occur when decision-making is dependent on computers or other automated aids, and the human is in an observatory role but able to make decisions [12]. Such deference to digital authority is increasingly problematic as humans integrate AI/ML decision makers into everyday life. Its impact is perhaps obvious in critical decision-making fields such as weapons control systems, but the effect of embedding such bias in widespread IoT – for example in recommender systems – could be debilitating.

The normative consequences of digital authoritarianism for the human rights of the individual are profound. The first proceeds from the location of authority in private commercial agents rather than in the state. The international human-rights architecture is constructed vertically: its instruments bind states and conceive of the individual as requiring protection principally against public power. The rights most obviously engaged by pervasive observation — the right to privacy under Article 7 of the Charter of Fundamental Rights of the European Union (CFREU), Article 8 of the European Convention on Human Rights (ECHR), and Article 12 of the Universal Declaration of Human Rights (UDHR) — were drafted against the spectre of state intrusion [8][11][45].

The articulation of Article 8 CFREU (“Protection of personal data”) was the first time a constitutional-level instrument expressly separated data protection from the older right to privacy and gave it standalone status. The moving force was the need to give constitutional permanence to a right that the Article 7 privacy guarantee could not adequately deliver in an era of automated data handling. What it seeks to protect is the individual’s informational self-determination — the fair, transparent and supervised processing of their personal data — as a right distinct from, though closely related to, private life.

A second implication arises from the consensual character of the regime, sustained as it is by data volunteered in exchange for benefit. The normative danger is that the idiom of voluntary exchange recasts a rights-impairment as an ordinary market transaction, thereby dissolving the claim that any right has been infringed at all. This is a pivotal move, for it shifts the question from whether rights are violated to whether they may be validly bartered — a question that engages the partial inalienability of fundamental rights.

Finally, there is the impact on freedom of speech. This is particularly acute, because the construct of digital authoritarianism cedes editorial power over public discourse to the platform. Where the dominant forums for political, civic and cultural expression are privately owned, the practical scope of speech is determined solely by the terms of service drafted unilaterally and enforced at scale by automated systems. The platform is thus a *de facto* regulator of expression, free to suppress lawful speech that no state would legitimately restrict and, conversely, to amplify or demote material on commercial rather than rights-based criteria. The normative upshot is that freedom of expression, conceived as a shield against the state, offers scant protection against a commercial sovereign whose control over the conditions of speech is more total, and less visible, than that which the right was designed to resist.

C. *Operational implications of digital authoritarianism*

Ceding authority to digital platforms raises practical issues of security and privacy. Since the IoT comprises billions of connected devices, the attack surface (the possible range of targets) is vastly expanded. Vulnerability is compounded by the fact that many IoT devices are not implemented with security in mind, perhaps because they perform non-sensitive tasks, or because they are designed for implementation within secure network perimeters and not intended for direct connection to web servers.

The broader issue is that apathy and deference to digital authority has inured many to data privacy infringement, and engendered data promiscuity. Data generated by intelligent agents may thus overwhelm flimsy safeguards for individual privacy that derive from the most fundamental common law and constitutional principles. In the light of these risks, the question of how digital authoritarianism and its enabling platform technologies are regulated and controlled becomes profoundly important. This challenge is addressed next.

V. REGULATING DIGITAL PLATFORMS

A. *Challenges with regulation of Digital Platforms*

Efforts to curtail the power of digital platforms can seem Sisyphean. Cohen describes a surveillance-innovation complex in which surveillance (and control) is ‘light, politically nimble and relatively impervious to regulatory constraint.’ [10] This is underscored by frequent infringements and grandstanding self-regulation on the part of digital platforms, and by weak enforcement by regulators. The progressive deployment of intelligent agents, AI and pervasive distribution intensifies the potential for harm.

At the same time, regulators suffer from structural disadvantages compared to digital platforms. Marsden talks of the Portarlington effect, a shorthand for the extreme inequality of arms between small national regulators and powerful digital corporations [24]. Regulators suffer from

informational and capability disadvantages compared to digital firms. They are poorly placed to conduct the constant monitoring required when proactive remedies are imposed, and they are exposed to the risk of regulatory capture. This frequently results in delayed investigation of infringement and lax or ineffective enforcement.

Nonetheless, legislators across several jurisdictions are attempting to curb the power of digital platforms. In Europe, under the banner of the Digital Single Market initiative, lawmakers have launched a significant programme of legislation that places significant obligations on large digital platforms, notably the Digital Services Act (DSA) and the Digital Markets Act (DMA) [17][18]. In the UK, the Online Safety Act (OSA) introduces liability for harm caused by specific digital firms [44]. Even in the US, where there has long been a broad interpretation of First Amendment rights, there have been moves to provide online privacy for citizens [7]. Digital platforms also conduct self-regulation by contractually setting norms or ‘house rules’ on their platforms. In this way they govern policy and usage and can take action against infringement, such as exclusion of a user.

These regulatory initiatives are taking place in the context of today’s challenges, even though the next wave of digital firepower is already here. The debate has already shifted, and the stakes considerably raised, by the widespread deployment of smart ubiquitous devices and machine learning technology.

B. *Possible models of regulation*

The complexity of the digital environment is engendered in part by the multiplicity of stakeholders involved. Digital platforms typically operate as multi-sided markets, and thus have many constituent actors (content providers, customers, advertisers, retailers, regulators and so on). Governance of intelligent agents used by these platforms will require a form of algorithmic regulation, an activity that necessarily requires cooperation of these various state and private actors, perhaps by adopting a model of decentered regulation.

Other proposals include regulating intelligent agents and their underlying algorithms along the lines of the pharmaceutical industry, using a central agency (the ‘FDA for algorithms’) to vet for safety and efficacy [43]. Marsden argues in favor of OffData, a new regulatory agency that ‘...draws on competition, technology regulation, fundamental human rights, privacy, and free expression to ensure a fair and neutral deal for digital prosumers and citizens [30]. In any scenario, given the pace, volatility and complexity of the digital environment, it is difficult not to envision the need for complex *dynamic* regulation as proposed by Murray [31].

There are calls also for international instruments building on shared principles of administrative law, which could resolve conflicts of law in the digital economy, although such initiatives might be difficult to achieve [29]. Regional attempts at regulation stand a better chance. For example, the EU’s AI Act applies to ‘AI systems used for indiscriminate

surveillance applied in a generalized manner to all natural persons without differentiation.’[16]. Such regulation does at least prohibit the use of intelligent agents in specified sensitive circumstances and introduces rules for AI systems designated as high risk.

VI. CONCLUSION AND FUTURE WORK

Large digital platforms are extending their influence over increasingly indifferent users who are willing to trade autonomy for convenience. This phenomenon, described here as digital authoritarianism, is enhanced by the widespread deployment of intelligent agents and risks undermining elected state authorities. It also places immense power in the hands of a small number of people. Addressing this democratic imbalance will require decentered dynamic regulation, taking account of the interests of all stakeholders rather than a simple binary mandate. Investigating suitable forms of regulation offers a substantive topic for future cross-disciplinary research.

There is scope also to explore further the constitutional implications touched on in this paper, specifically to assess the robustness of regulatory instruments as a shield for human rights. Equally, the inevitability of digital authoritarianism and the uniformity of user deference posited in this research is likely to promote diverse user practices and resistance which warrant further investigation.

REFERENCES

- [1] H. Arendt, ‘The Origins of Totalitarianism’, 1966, 3rd ed., Harcourt Brace.
- [2] Article 29 Data Working Party: Opinion 8/2014 on Recent Developments on the IoT, 2014
- [3] J. Bentham, “Panopticon writings”, (M. Bozovic, Ed.). Verso, (Original work published 1787)
- [4] A. Bradford, “Europe’s Digital Constitution”, *Virginia Journal of International Law*, 2023, Vol.64, Iss. 1, pp. 1-68
- [5] D. N. Cicilline, Opening statement at hearing on “Online Platforms and Market Power, Part 6, U.S. House of Representatives Antitrust, Commercial, and Administrative Law Subcommittee. (2020, July 29) <https://cicilline.house.gov/press-release/cicilline-opening-statement-at-big-tech-antitrust-hearing> (retrieved: June, 2026)
- [6] R. Calo, “Robotics and the Lessons of Cyberlaw”, W. Barfield and U. Pagallo (eds) “Research Handbook on the Law of Artificial Intelligence”, Edward Elgar, Cheltenham, 2018
- [7] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (2018)
- [8] Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391
- [9] A. Chatfield and C. Reddick, “A framework for Internet of Things-enabled smart government”, *Government Information Quarterly*, 2019, Vol. 36, pp. 346–357
- [10] J. Cohen, “Between Truth and Power”, Oxford University Press, NY, 2019
- [11] Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), 213 UNTS 221 (1950)
- [12] D. Danks and A. London, “Algorithmic Bias in Autonomous Systems”, *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17)*, 2017
- [13] DataReportal, We Are Social, and Meltwater, 2025, Number of connected devices worldwide as of October 2025, Statista. <https://www.statista.com/statistics/1559435/connected-devices-worldwide/> (retrieved: March, 2026)
- [14] R. Diebert, “Authoritarianism goes Global: Cyberspace under Siege”, *Journal of Democracy*, 2015, Vol. 26, No. 3, pp. 64-78
- [15] G. Dyson, “Turing’s Cathedral”, Penguin Books, London, 2012, p.308
- [16] European Parliament & Council of the EU, Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024, OJEU
- [17] European Parliament & Council of the EU, Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act), 2022, OJEU
- [18] European Parliament & Council of the EU, Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act), 2022, OJEU
- [19] L. Floridi, “The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU”, *Philosophy & Technology*, 2020, Vol. 33, pp. 369–378
- [20] M. Foucault, “Discipline and Punish: The Birth of the Prison”, 1977, (trans. A. Sheridan), Pantheon Books
- [21] M. Gal, “Algorithmic Challenges to Autonomous Choice”, *Michigan Telecommunications and Technology Law Review*, 2017, <http://dx.doi.org/10.2139/ssrn.2971456> (retrieved: March, 2026)
- [22] Granma: <http://en.granma.cu/mundo/2019-06-07/digital-totalitarianism/> (retrieved: March, 2026)
- [23] M. Hildebrandt, “Law as Information”, *Modern Law Review*, 2016, Vol. 79, Issue 1, pp 1-30
- [24] House of Lords Communications Committee, “Regulating in Digital World” – oral & written evidence”, p.906- 934 [theadvertisingindustry \(parliament.uk\)](https://www.parliament.uk/business/committees/committees-a-z/commons-secondary/communications-committee/written-evidence/) (retrieved: February, 2026)
- [25] N. Howe, “The Rise of Totalitarian Technology”, *Forbes*, 2019, <https://www.forbes.com/sites/neilhowe/2019/03/06/the-rise-of-totalitarian-technology/> (retrieved: March, 2026)
- [26] IoT Analytics, 2024, Number of connected IoT devices growing 13% to 18.8 billion globally, Statista. <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/> (retrieved: March, 2026)
- [27] N. Kobie, “The Complicated Truth about China’s Social Credit System”, *Wired*, 2019 <https://www.wired.co.uk/article/china-social-credit-system-explained> (retrieved: March, 2026)
- [28] B. J. Koops, “The trouble with EU DP law”, *International Data Privacy Law*, 2014, Vol. 4, No. 4, pp. 250-261
- [29] E. Marique and Y. Marique, “Sanctions on Digital Platforms - Beyond the Public/Private Divide”, *Cambridge International Law Journal*, 2019, vol. 8., Issue. 2, pp. 258 – 281
- [30] C. Marsden, “Prosumer law and network platform regulation”, *Georgetown Law Technology Review*, Vol. 2, Issue 2 2018 pp. 376-398
- [31] A. Murray, “Mapping the Cyber-Regulatory Environment”, Routledge, London, 2006
- [32] NHS Data Blog, “NHS still reliant on paper notes and drug charts despite electronic upgrades - BMJ Group”, (retrieved: March, 2026)
- [33] K. O’Hara, K and N. Shadbolt, “The right to be forgotten”, *European Data Protection Law Review*, 2015, Vol. 1, Issue 3, pp. 178-189
- [34] G. Orwell, “1984”, Secker & Warburg Ltd., London, 1949
- [35] F. Pasquale, “From Territorial to Functional Sovereignty”, *LPE Blog*, 2017, *From Territorial to Functional Sovereignty: The Case of Amazon - LPE Project* (retrieved: March, 2026)

- [36] F. Pasquale, “The Black Box Society”, Harvard University Press, 2016
- [37] I. Rubinstein, “Big Data: The End of Privacy or a New Beginning?”, New York University Public Law and Legal Theory Working Papers, Paper 357, 2012
- [38] P. Sales, “Algorithms, artificial intelligence and the law”, Sir Henry Brooke Lecture for BAILII, 2019, British and Irish Legal Information Institute (BAILII)
- [39] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, “Modernising the law on abuse of market power: Report for the Federal Ministry for Economic Affairs and Energy (Germany)”, Federal Ministry for Economic Affairs and Energy (BMWi), 2018
- [40] Stanford University, “100 year Study on AI”, <https://ai100.stanford.edu> (retrieved: March, 2026)
- [41] Stigler Committee on Digital Platforms, Policy Brief, Stigler Centre, 2019, p.2
- [42] C. Sunstein and R. Thaler, “Libertarian Paternalism is not an Oxymoron”, University of Chicago Public Law & Legal Theory Working Paper No. 43, 2003, Libertarian Paternalism Is Not an Oxymoron (retrieved: March, 2026)
- [43] A. Tutt, “An FDA for Algorithms”, 69 Administrative Law Review 83, 2017 pp. 83-123
- [44] UK Parliament, Online Safety Act 2023, The Stationery Office, <https://www.legislation.gov.uk/ukpga/2023/50>, (retrieved: March, 2026)
- [45] Universal Declaration of Human Rights, UNGA Res 217 A(III) (1948)
- [46] R. Van Loo, “The Corporation as Courthouse”, Yale Journal on Regulation, 2016, Vol. 33, Iss. 2, p. 547
- [47] K. Yeung, “Algorithmic Regulation: a critical interrogation”, Regulation and Governance, 2017, Vol. 12, pp. 505–523
- [48] K. Yeung, “‘Hypermudge’: Big Data as a mode of regulation by design”, Information, Communication & Society, 2017, Vol. 20, No. 1, pp. 118–136
- [49] S. Zuboff, “The Age of Surveillance Capitalism”, Profile Books, London, 2019