International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

When Rights Cannot Be Used: Defensive Sovereignty, Privacy, and the Operational Conditions of Citizenship

Elias Rubenstein

Independent Researcher, Fort Lauderdale, FL, USA
ORCID: 0009-0007-1956-653X

Abstract

This paper extends the framework of conditionalized sovereignty [1] from permission-based autonomy to defensive sovereignty. While conditionalized sovereignty explains how formally recognized autonomy may become dependent on permission, defensive sovereignty examines whether citizens retain the operational capacities required to defend rights against arbitrary power. The central argument is that rights are not secure merely because they are formally declared; they require usable infrastructures, procedures, remedies, privacy protections, financial access, communicative channels, educational plurality, legal recognition of caregiving and family-like arrangements, and contestable decision-making systems. The paper introduces the concepts of operational citizenship, rights-disabling, hybrid power, function creep, assessment capture, relational rights-disabling, and resilient sovereignty safeguards. Drawing on legal, political-theoretical, human-rights, artificial intelligence (AI) governance, property-rights, emergency-powers, and policy-capture literature, it analyzes selected domains of modern civic life in which rights may remain formally intact while becoming operationally fragile. It concludes with the Resilient Sovereignty Safeguards Test, a diagnostic framework for assessing whether rights remain usable when the infrastructures required to exercise and defend them are controlled, weakened, or made dependent on discretionary permission.

Keywords: Defensive Sovereignty, Operational Citizenship, Privacy, Infrastructural Power, Rights-Disabling

1. Introduction: From Conditionalized Sovereignty to Defensive Sovereignty

This paper extends the framework of conditionalized sovereignty [1]. That framework argues that modern legal systems may preserve formal autonomy while conditioning its practical exercise through permission, compliance, administration, institutional recognition, fiscal visibility, medical authorization, property regulation, inherited assumptions, and moral governance. Its central concern is the asymmetry of legal maturity: citizens are often treated as fully mature for obligation, taxation, liability, punishment, labor, debt, and compliance, while being treated as only conditionally mature in domains of self-regarding autonomy such as body, health, property, conscience, risk, family life, and existential self-direction [1].

The present paper develops the next step. Conditionalized sovereignty explains how rights-exercise becomes permission-based. Defensive sovereignty explains how rights-defense becomes operationally disabled. Together, the two frameworks describe connected stages of modern sovereignty loss: first, citizens may need permission to act; second, they may lose the practical means to contest, resist, or defend against that permission structure.

Modern legal systems commonly describe citizens as free, responsible, rights-bearing, property-owning, privately secure, educationally protected, and politically represented. Yet the exercise of these rights increasingly depends on infrastructures, platforms, financial systems, administrative procedures, digital identities, educational institutions, expert regimes, emergency powers, and algorithmic classifications.
A citizen may formally possess freedom of speech while losing visibility through platform moderation or algorithmic de-ranking. A citizen may formally possess privacy while being subjected to generalized surveillance or weakened encryption. A citizen may formally possess property while facing majoritarian extraction, confiscatory taxation, or regulatory takings. A citizen may formally possess financial autonomy while being excluded from banking or payment systems. A citizen may formally possess parental educational rights while lacking any meaningful alternative to state-defined curricula or assessment regimes. A citizen may formally possess private and family life while losing protection because a relational or household arrangement does not match the state's preferred model. A citizen may formally possess due process while automated systems deny explanation, review, or remedy.

The central claim is therefore:

Formal rights are insufficient when the operational conditions required to exercise and defend them can be controlled, disabled, surveilled, censored, automated, financialized, monopolized, or dismantled by the same powers they are meant to restrain.

This paper does not reject regulation, public safety, democratic government, education, technology, expertise, family law, or lawful criminal investigation. It distinguishes legitimate regulation directed at concrete harm from arrangements that weaken the operational conditions of rights beyond what is necessary, proportionate, transparent, reviewable, and publicly justified.

2. Method, Scope, and Original Contribution

2.1 Method and Scope

This paper uses conceptual legal and political-theoretical analysis. It does not provide a jurisdiction-specific doctrinal survey, an empirical study, or a comprehensive comparative account of every legal system mentioned. Its purpose is to identify a recurring structural vulnerability: rights may remain formally recognized while the operational conditions required to use them are controlled by public, private, hybrid, or algorithmic power.

The breadth of the paper is methodological rather than doctrinal. The selected domains are not exhaustive legal surveys, but illustrative cases of one structural phenomenon: operational rights-disabling. They were selected because they cover major conditions of modern civic life: formation and education, private and

family life, property, financial access, communication, technological mediation, epistemic authority, emergency governance, and lawful defensive capacity.

The paper proceeds in four steps. First, it defines the central concepts of defensive sovereignty, operational citizenship, rights-disabling, hybrid power, function creep, assessment capture, relational rights-disabling, resilient sovereignty safeguards, and arbitrary power. Second, it situates the argument within republican non-domination theory, liberal harm theory, rule-of-law theory, privacy and human-rights law, business-and-human-rights principles, AI governance, educational-rights doctrine, family-life jurisprudence, policy-capture literature, property theory, emergency-powers theory, and criminal-law/self-defense doctrine. Third, it applies the framework to selected operational domains of citizenship. Fourth, it introduces the Resilient Sovereignty Safeguards Test as a diagnostic tool for evaluating whether rights are protected not only in formal doctrine, but in practical operation.

2.2 Relevance

The framework is relevant to legal theory, constitutional analysis, digital governance, civil liberties, educational rights, family law, financial inclusion, and emergency-powers scholarship. Its value lies in shifting analysis from formal rights to the infrastructural, procedural, financial, educational, relational, and technological conditions that make those rights usable.

This shift is especially important where majority approval, administrative convenience, platform governance, financial exclusion, curricular monopoly, family-form restriction, emergency rhetoric, or algorithmic classification can affect the practical availability of rights without openly abolishing them.

2.3 Original Contribution

Existing literature has examined liberty, privacy, platform power, artificial intelligence governance, property rights, family rights, educational rights, policy capture, emergency powers, financial exclusion, digital authoritarianism, and self-defense separately. This paper integrates these domains into a single framework: defensive sovereignty as the operational architecture that makes rights usable against arbitrary power.

The contribution is not the claim that each domain is new. Rather, the contribution lies in identifying a shared structure:

Rights may remain formally recognized while their operational conditions are captured, conditioned, automated, centralized, financialized, surveilled, monopolized, or made dependent on discretionary permission.

The paper is therefore not a catalogue of policy complaints. It is a conceptual theory of operational rights-disabling. Its originality lies in treating rights-disabling as a cross-domain legal and political-theoretical structure rather than as a problem confined to any single field of regulation.

3. Theoretical Background: From Non-Domination to Operational Rights

The conceptual foundation of this paper lies in the distinction between formal liberty and freedom from arbitrary power. Contemporary republican theory understands liberty not merely as non-interference, but as non-domination, that is, independence from arbitrary power [2-5]. Domination may exist even where no direct interference has yet occurred. A person may remain formally free while living under a power that can interfere at will, without sufficient justification, contestability, or accountability [2-5].

Classical liberal and harm-based theories further support the distinction between legitimate regulation aimed at preventing harm and paternalistic or moralizing restrictions that exceed the justification of concrete injury to others [6-8]. Defensive sovereignty builds on this distinction. It does not deny regulation. It asks whether regulation remains connected to concrete harm, proportionality, review, and public justification, or whether it disables the operational conditions of rights beyond what is necessary.

In contemporary legal orders, arbitrary power is no longer exercised only through direct command, prohibition, or punishment. It may also operate through infrastructures that determine whether rights can be used in practice: communication networks, platforms, banking systems, digital identities, artificial intelligence, educational accreditation, expert standards, administrative classifications, family-status categories, and emergency frameworks.

Rule-of-law theory reinforces this point. The rule of law is not satisfied by formal legality alone. It requires legality, legal certainty, prevention of abuse of power, equality before the law, access to justice, checks and balances, and meaningful review [9-12]. A right that cannot be contested, reviewed, or remedied is therefore not fully operational, even if it remains formally recognized. This is especially important when decision-making is automated or opaque, because technological due-process scholarship has shown that automated administrative decisions may undermine rights if reasons, review, and correction mechanisms are absent [36].

Privacy and freedom of expression also require operational conditions. International and European human-rights frameworks protect private life, family life, home, and correspondence, while the United Nations (UN) Special Rapporteur on freedom of opinion and expression has treated encryption and anonymity as connected to privacy and freedom of expression in digital communication [13,15,17,22]. Privacy scholarship similarly shows that privacy is not merely secrecy but a condition for self-development, association, intellectual life, and protection from invasive social ordering [20,21].

The same logic applies to chilling effects. A right may be weakened before any formal prohibition occurs if citizens anticipate monitoring, punishment, reputational damage, financial exclusion, or algorithmic classification. Legal scholarship on surveillance and chilling effects has argued that surveillance may affect speech and intellectual inquiry by inducing self-censorship, conformity, or anticipatory withdrawal from lawful conduct [18,19].

Modern rights-disabling often operates through hybrid power rather than a single identifiable state actor. Public authorities, private platforms, financial intermediaries, corporations, expert bodies, educational systems, family-law structures, and algorithmic systems may jointly structure access, visibility,

legitimacy, and opportunity. Internet shutdown reports, platform-governance scholarship, and business-and-human-rights principles show that public-private infrastructures can shape rights without a single transparent decision-maker [23-28].

Policy-capture and regulatory-capture literature further explains how public decisions may be redirected by special interests, lobbying, funding structures, expert networks, or institutional incentives [29-32,40]. This matters because expertise can become a form of governance when technical language, soft law, standards, metrics, and advisory frameworks shape public policy without sufficient democratic accountability.

The theoretical bridge can therefore be stated as follows:

Rights are protected not only when they are declared, but when citizens retain the operational capacities, institutional remedies, infrastructural access, and contestable procedures required to use them.

The argument proceeds in six steps. Conditionalized sovereignty first shows how autonomy may remain formal while its exercise becomes permission-based [1]. Defensive sovereignty then asks whether rights remain usable when the conditions of their exercise are controlled. Rights-disabling occurs where the right remains legally intact but the means of using it are weakened. In modern legal orders, this disabling often operates through hybrid power, function creep, automation, surveillance, financial exclusion, educational monopoly, relational exclusion, and lack of remedy. Rights must therefore be evaluated not only doctrinally, but operationally. The Resilient Sovereignty Safeguards Test provides a structured method for that evaluation.

4. Conceptual Framework

4.1 Defensive Sovereignty

Defensive sovereignty refers to the practical, institutional, infrastructural, financial, procedural, relational, epistemic, and physical capacities through which citizens can protect themselves against arbitrary power, majority abuse, private coercion, infrastructural dependency, formative monopoly, relational exclusion, and state overreach.

The concept does not imply absolute independence from law. It describes the minimum conditions under which citizenship remains practically meaningful. Citizens are not defensively sovereign merely because rights are declared in legal texts. They are defensively sovereign when they retain the practical means to invoke, use, contest, communicate, finance, educate, associate, and defend those rights.

4.2 Operational Citizenship

Operational citizenship means that citizenship is not merely a formal legal status, but a practical condition requiring usable rights, remedies, privacy, property, communication, financial access, educational plurality, relational protection, contestability, and lawful defensive capacity.

A right to speech requires access to communication channels and protection against arbitrary visibility control [23-26]. A right to privacy requires confidentiality, encryption, and limits on generalized surveillance [13,15,17,20-22]. A right to property requires title and protection against arbitrary confiscation, disproportionate taxation, and majoritarian extraction [50-52]. A right to education requires access to instruction without monopolized formative control [14-16,41-44]. A right to private and family life requires mechanisms that prevent lawful adult relational choices from becoming practically unprotected [15,22,45-49]. A right to due process requires reasons, review, appeal, and enforceable remedy [9-12,36].

4.3 Rights-Disabling

Rights-disabling occurs when a right remains formally recognized while the practical conditions required to exercise it are restricted, centralized, automated, surveilled, deplatformed, financialized, monopolized, or made dependent on discretionary permission.

Speech may be weakened through de-ranking, demonetization, reputational labeling, or search suppression [25,26]. Privacy may be weakened through bulk access, generalized scanning, or encryption backdoors [13,17,20-22]. Property may be weakened through regulatory burdens or politically convenient expropriation [50-52]. Financial autonomy may be weakened through debanking, account freezes, or exclusion from payment systems [53-55]. Educational autonomy may be weakened through curricular monopoly or assessment capture [14-16,41-44]. Relational autonomy may be weakened when adults are formally free to choose non-standard household or caregiving arrangements while losing the legal protections attached to recognized family forms [15,22,45-49]. Due process may be weakened through automated decisions that provide neither reasons nor meaningful appeal [33-39].

Rights-disabling may also occur through chilling effects. When citizens know that communication, payment behavior, search activity, association, lawful dissent, educational choices, relational arrangements, or movement may be monitored, profiled, punished, or algorithmically classified, they may refrain from lawful conduct before any formal restriction occurs [18,19].

4.4 Hybrid Power

Modern rights-disabling often occurs through hybrid power: public authority, private platforms, financial intermediaries, educational institutions, expert bodies, family-law structures, and algorithmic systems operating together without a single accountable decision-maker [23-32,40].

Traditional legal accountability often assumes an identifiable state actor or a clearly reviewable administrative decision. Hybrid power blurs responsibility. A government may pressure platforms; platforms may enforce opaque rules; banks may act under compliance expectations; AI systems may classify risk; educational authorities may define mandatory content; expert bodies may shape policy standards; family-law categories may determine access to protection; and citizens may face consequences without knowing where the actual decision originated.

4.5 Function Creep

Function creep occurs when an infrastructure introduced for one limited purpose is later expanded to other domains, populations, risks, or political objectives.

Financial monitoring introduced for money laundering may expand into political-risk classification [55]. Emergency tools may become general behavioral-governance tools [56-58]. Educational standards introduced to prevent neglect may expand into worldview standardization [14-16,41-44]. Family-status rules introduced for administrative clarity may become exclusionary gates to protection [45-49]. AI systems introduced for efficiency may become eligibility and exclusion mechanisms [33-39]. Function creep matters because the original justification may be narrow, while the later infrastructure becomes broad, permanent, and difficult to dismantle.

4.6 Assessment Capture

Assessment capture occurs when alternative education remains formally available, but its legal recognition, continuation, or social validity depends on examinations or evaluative standards that reproduce the state's preferred curriculum, worldview, or interpretive framework [14-16,41-44].
This does not mean that all examinations are illegitimate or that educational competence cannot be assessed. The issue is whether minimum competence is defined so narrowly through a state-monopolized formative framework that alternative education becomes formally permitted but practically dependent on reproducing the same underlying assumptions.

4.7 Relational Rights-Disabling

Relational rights-disabling occurs when lawful adult relational, household, caregiving, or family-like arrangements remain formally tolerated but are deprived of the legal protections necessary to make them stable, defensible, and secure [15,22,45-49].

The issue is not whether the state may define marriage or regulate family status. It may. The issue is whether a preferred relational model becomes the sole gateway to basic protection of adult intimacy, caregiving, household interdependence, medical decision-making, inheritance, property sharing, and family-like responsibility.

4.8 Resilient Sovereignty Safeguards

Resilient sovereignty safeguards are protections designed to remain effective when political, administrative, financial, educational, relational, platform-based, epistemic, or algorithmic power attempts to weaken them.

Such safeguards include due process, judicial review, transparency requirements, appeal rights, purpose limitation, sunset clauses, compensation requirements, anti-capture rules, cash protection, analog access, encryption, educational plurality, relational protection, decentralized infrastructure, and lawful defensive capacity.

The central formula is:

A right is not sufficiently protected if it can be disabled by the same authority or infrastructure it is meant to restrain.

4.9 Arbitrary Power

Arbitrary power refers to power that affects the citizen's rights or operational capacities without sufficient public justification, transparency, proportionality, due process, contestability, or independence from private, political, educational, relational, or institutional capture [2-12,29-32,40].

This definition avoids reducing arbitrariness to illegality alone. A measure may be formally legal while still being arbitrary in operation if it lacks transparent justification, meaningful review, proportionate scope, or independence from capture.

Each following domain is analyzed through the same logic: a formal right, an operational condition, a disabling mechanism, and a resilient safeguard.

5. Due Process as Defensive Infrastructure

Due process is the procedural form of defensive sovereignty. Without reasons, review, and remedy, rights become dependent on administrative discretion.

A right becomes fragile when citizens cannot know why they were excluded, flagged, debanked, deplatformed, surveilled, algorithmically classified, denied service, deprived of property, denied educational recognition, denied relational protection, or restricted in lawful defensive capacity. In such cases, the right may formally exist, but the citizen lacks the procedural means to defend it.

Due process requires notice, reasons, access to relevant information, the opportunity to be heard, independent review, appeal, proportionality, burden of justification on the restricting authority, and enforceable remedy. Where a decision affects core conditions of civic life--communication, property, banking, education, relational status, identity, employment, mobility, public services, reputation, or legal status--the need for meaningful due process becomes stronger [9-12,36].

The problem is especially acute where decision-making is automated, outsourced, privately mediated, or hidden behind institutional discretion. If an algorithm denies access, a platform suppresses visibility, a bank closes an account, an educational authority refuses recognition, a legal system denies standing to a household arrangement, or an administrative system flags a citizen as a risk without explanation, the citizen may be unable to contest the decision in any meaningful way [33-39].

The central principle is:

A right without a forum and enforceable remedy is a declaration, not an operational protection.

6. Privacy, Family Life, Security Exceptions, and the Generalization of Suspicion

6.1 Privacy as the Inner Domain of Defensive Sovereignty

Privacy is the inner domain of defensive sovereignty. It protects the citizen's self-regarding life from permanent exposure, prediction, suspicion, and administrative interpretation.

Privacy is not merely data protection. It is the protected space in which citizens may live, think, read, research, correspond, move, associate, educate, form relationships, and make lawful self-regarding choices without constant justification [13,15,17,20-22]. It includes the home, correspondence, body, personal habits, intellectual exploration, relationships, encryption, anonymity, and protection against generalized suspicion [13,15,17,22].

The central principle is:

Citizens do not need to justify why private life should remain private. The state must justify why it seeks access.

Privacy also protects dissent before dissent becomes public. Without private communication, private reading, confidential association, family autonomy, and relational privacy, citizens may censor themselves before any formal censorship occurs [18,19].

6.2 Relational Sovereignty and the Conditional Protection of Family Forms

Privacy also includes the relational domain of adult life. A legal order shapes private life not only through surveillance or bodily regulation, but also by deciding which forms of intimacy, household organization, caregiving, partnership, and family receive legal recognition and protection [15,22,45-49].

This paper does not argue that every relational form must be treated identically in every legal domain. Nor does it argue for the abolition or devaluation of classical marriage. Legal systems may legitimately require clarity in matters of inheritance, parentage, taxation, immigration, medical decision-making, property, duties of care, and protection of vulnerable persons. The argument concerns basic protective instruments for functional adult caregiving communities: medical authorizations, inheritance planning, property protection, tenancy security, caregiving recognition, and legal standing where adults have created durable bonds of mutual responsibility. The issue is not whether every relationship becomes marriage. The issue is whether lawful adult forms of care and household interdependence are left legally defenseless merely because they do not match one state-preferred model.

The problem arises when protection of basic relational interests becomes narrowly tied to a single state-preferred family form. Adults may be free to live in non-standard, non-marital, communal, religious, philosophical, caregiving-based, or alternative household arrangements, yet lose access to protections that make intimate and family life legally secure. They may face difficulties in hospital visitation, medical decision-making, inheritance, tenancy, parental recognition, taxation, insurance, property sharing, caregiving recognition, or legal standing. The state does not necessarily prohibit the relationship. It simply withholds the protective infrastructure attached to recognized family forms.

The central principle is:

A private relationship is not meaningfully free if choosing it requires losing the legal protections that make private life defensible.

Necessary safeguards include contractual recognition of caregiving arrangements, medical-decision authorizations, inheritance planning mechanisms, tenancy and household protections, legal tools for property sharing, and reviewable pathways for recognizing family-like responsibilities without forcing all relationships into one marital model.

6.3 Security Exceptions and Generalized Suspicion

Serious harms such as terrorism, child abuse, organized crime, violence, cybercrime, and money laundering are real. They may justify targeted, lawful, evidence-based, reviewable interventions. They do not justify generalized permanent access infrastructures that weaken privacy for all citizens [7,13,15,17,20-22,55].

The distinction is between targeted investigation and generalized suspicion. Targeted investigation begins from concrete suspicion, lawful authority, proportionality, and review. Generalized suspicion begins from the assumption that the population must be searchable, scannable, predictable, and permanently available to inspection because serious crimes exist somewhere.

The existence of serious crime does not create a general warrant for permanent access to private life. The state may investigate concrete wrongdoing. It may not convert the entire citizenry into a permanently searchable population.

Necessary safeguards include judicial warrants, concrete suspicion, proportionality, purpose limitation, prohibition of bulk surveillance, prohibition of general backdoors, independent oversight, transparency reports, sunset clauses, and sanctions for misuse.

7. Property and Material Independence Against Majority Power

Property is not merely an economic asset; it is a material condition of personal sovereignty [50-52].

A person without secure property is more dependent on state discretion, administrative permission, employers, banks, licensing systems, welfare structures, political favor, and majority approval. Property creates practical space for independence. It supports the ability to dissent, relocate, publish, work, build, fund litigation, educate independently, protect lawful household arrangements, resist pressure, and avoid total dependency on institutions [50-52].

This argument does not deny taxation, redistribution, or land-use regulation as such. It asks when such measures become disproportionate, punitive, retroactive, or targeted in ways that transform property from a protected right into a politically available resource.

The central principle is:

Democratic enactment alone does not settle the justice of majoritarian interference with protected property interests.

The relevant distinction is not between property and public interest. The distinction is between proportionate public regulation and arbitrary material dispossession.

Necessary safeguards include constitutional property guarantees, compensation requirements, judicial review, proportionality, protection against retroactive confiscation, limits on punitive taxation, clear public-use or public-interest standards, minority protection, and a high burden of justification for severe property interference.

8. Infrastructural Sovereignty: Communication, Platform Visibility, and Financial Access

8.1 Communicative and Informational Sovereignty

Citizens cannot defend rights that they cannot communicate, document, coordinate, publish, or make visible.

Communication is protective infrastructure. Through communication, citizens document abuse, contact counsel, organize assistance, reach journalists, inform international audiences, coordinate lawful protest, preserve evidence, and maintain educational, cultural, or relational alternatives. When communication infrastructure is disabled, rights may remain formally intact while becoming operationally unusable [23-26].

A state that can switch off communication can severely impair citizenship without formally suspending rights.

Internet shutdowns demonstrate how communication infrastructure can become a condition of operational citizenship. Access Now and the #KeepItOn coalition documented 296 shutdowns in 54 countries in its 2024 report and 313 shutdowns in 52 countries in its 2025 report [23,24]. Such measures may not abolish rights in legal language, but they can incapacitate rights in practice by cutting off documentation, coordination, publication, access to counsel, and public visibility.

Modern censorship also need not prohibit speech directly. It can control reach, visibility, reputation, and monetization. Platform moderation, state-platform pressure, shadowbanning, de-ranking, demonetization, labeling, search suppression, and algorithmic visibility control can weaken speech without formally banning it [25,26]. Platform governance illustrates hybrid power: private entities structure visibility and access, while public pressure, regulation, or informal coordination may shape moderation practices without a single transparent decision-maker [23-28].

Necessary safeguards include judicial control of network restrictions, emergency communication rights, protection of virtual private networks (VPNs) and encryption, decentralized infrastructure, transparency

of government takedown requests, appeal rights for deplatforming, interoperability, data portability, and protection of independent media.

8.2 Financial Sovereignty and Economic Exclusion

In a digital economy, financial access is not a convenience; it is a condition of practical citizenship [53-55].

Citizens who can be financially disconnected can be socially neutralized without being formally punished. Banking access, payment processing, credit, insurance, and the ability to transact are increasingly necessary for ordinary civic life. Without them, people may be unable to work, rent, travel, publish, receive donations, operate a business, pay legal fees, fund independent education, or sustain basic economic participation.

Financial exclusion may occur through debanking, account closure, payment processor exclusion, credit and insurance scoring, asset freezes, programmable money restrictions, financial surveillance, compliance pressure, or politically sensitive risk classifications. Some financial restrictions are justified where fraud, money laundering, terrorism financing, or crime is present. The issue is whether such mechanisms remain targeted, reviewable, and proportionate--or whether they become tools of non-criminal exclusion [53-55]. In the European context, the Payment Accounts Directive recognizes access to a basic payment account as a legal concern rather than a mere consumer convenience [53]. Financial-surveillance scholarship also shows how anti-terrorism and anti-money-laundering infrastructures may expand into broader risk-governance systems [55].

Necessary safeguards include a right to basic banking, reasons for account closure, appeal rights, anti-discrimination rules, cash protection, payment plurality, judicial review before asset freezes, due process before account blocking, and a clear separation between crime prevention and political or reputational exclusion.

9. AI-Mediated Sovereignty and Automated Permission

Artificial intelligence does not merely automate decisions; it can automate permission. Here, permission means practical access to visibility, services, eligibility, mobility, credit, employment, reputation, and institutional recognition.

AI becomes a sovereignty issue when it determines access to essential conditions of civic life: visibility, credibility, credit, insurance, employment, mobility, public services, reputation, security classification, health prioritization, education, relational recognition, and political reach. Citizens may not be directly prohibited from acting, but they may be classified, ranked, filtered, predicted, deprioritized, excluded, or flagged by systems they cannot inspect or contest [33-39].

AI should be distinguished across three levels. First, AI may support human decision-making. Second, AI may function as an access gatekeeper by determining eligibility, visibility, risk status, or priority. Third, AI may become a behavioral-governance system by shaping incentives, discouraging lawful conduct, filtering information, or predicting future risk. The sovereignty problem begins most clearly at the second

and third levels, where AI systems no longer merely assist decisions but structure the conditions of access, visibility, credibility, and participation [33-39].

The European Union (EU) Artificial Intelligence Act (AI Act) treats certain AI practices as prohibited because of fundamental-rights risks, including harmful manipulation, exploitation of vulnerabilities, social scoring, certain criminal-risk prediction practices, and emotion recognition in workplaces and educational institutions [33]. As the AI Act moves from enactment toward practical application, this concern becomes especially relevant for access-gatekeeper systems. AI systems used in areas such as education, employment, access to essential services, law enforcement, migration, and administration of justice may fall within high-risk categories where providers and deployers face duties concerning risk management, data governance, documentation, transparency, human oversight, accuracy, robustness, and post-market monitoring [33]. This supports the present argument: when AI systems mediate access to core conditions of civic life, they should not be treated as ordinary technical tools, but as operational infrastructures of rights.

The National Institute of Standards and Technology (NIST) AI Risk Management Framework treats AI risk as potentially affecting individuals, organizations, and society, while the United Nations Educational, Scientific and Cultural Organization (UNESCO) framework on the ethics of artificial intelligence emphasizes human rights, transparency, accountability, fairness, and oversight [34,35]. Scholarship on technological due process, automated inequality, sociotechnical fairness, and machine-learning governance further supports the claim that AI cannot be treated as merely technical infrastructure [36-39].

The danger is not only that AI systems may make mistakes. The deeper danger is that AI may become an invisible administrative layer through which permission, exclusion, reputation, and opportunity are distributed without meaningful transparency, appeal, or human accountability.

The central principle is:

A decision that cannot be explained cannot be meaningfully contested.

Necessary safeguards include explanation, human review, independent audits, transparent classification criteria, prohibition of social scoring, prohibition of covert political manipulation, data minimization, no fully automated exclusion from essential services, liability for harmful automated decisions, and public oversight of government AI systems.

10. Educational Sovereignty, Assessment Capture, and Curricular Control

Education is an operational condition of citizenship. A legal order shapes citizens not only through law, taxation, policing, platforms, financial systems, or artificial intelligence, but also through compulsory schooling, curricula, accreditation, examinations, testing standards, and the institutional definition of legitimate knowledge [14-16,41-44].

The argument does not deny the state's legitimate interest in basic competence, child welfare, and prevention of educational neglect. It challenges only the conversion of educational oversight into formative monopoly.

Compulsory education may serve legitimate purposes. A state may require literacy, numeracy, civic knowledge, and protection from neglect. The problem arises when oversight moves from minimum competence into formative monopoly: when the state does not merely require education, but controls the range of permissible knowledge, historical narratives, moral assumptions, social doctrines, and evaluative standards through which children must be formed.

This problem becomes especially visible through examinations and assessment regimes. Even where alternative education, private schooling, religious schooling, homeschooling, or hybrid education is formally permitted, such alternatives may remain operationally weak if recognition depends on a single state-defined curriculum or examination framework. The state need not prohibit alternatives directly. It can make them dependent on state-approved testing standards, mandatory content, approved learning outcomes, and official definitions of knowledge.

This paper calls this assessment capture.

Assessment capture occurs when alternative education remains formally available, but its legal recognition, continuation, or social validity depends on examinations or evaluative standards that reproduce the state's preferred curriculum, worldview, or interpretive framework. Standardized tests rarely measure competence in a purely neutral vacuum. Even when presented as objective assessment, they may embed assumptions about history, civic identity, social norms, moral vocabulary, scientific interpretation, cultural authority, and legitimate forms of reasoning. The danger is not educational evaluation as such. The danger is that recognition may depend on reproducing the interpretive frame of a state-defined curriculum. Assessment then ceases to measure minimum competence and becomes a mechanism of formative alignment.

Educational-rights doctrine recognizes education as a domain of state interest, child development, parental responsibility, conscience, and philosophical conviction rather than merely an administrative service [14-16,41-44]. Article 26 of the Universal Declaration of Human Rights states that parents have a prior right to choose the kind of education given to their children [14]. Article 2 of Protocol No. 1 to the European Convention protects the right to education while requiring respect for parents' religious and philosophical convictions [15,16]. United States (U.S.) constitutional cases such as Meyer, Pierce, and Yoder illustrate the legal significance of parental direction and religious or philosophical educational claims, while Konrad v. Germany shows that some legal systems may uphold strict compulsory-schooling regimes [41-44]. The point is not that parental choice is absolute. The point is that education is a protected field of family life, conscience, philosophical conviction, and intergenerational formation, not merely an administrative service.

Educational sovereignty is operationally disabled when parents formally retain family rights, religious freedom, or conscience rights, but practically lack any meaningful alternative to state-approved formative

instruction. It is also disabled when alternative education is permitted in name but made dependent on examinations that require contested ideological content rather than neutral competence.

The central principle is:

A child's right to education should not be transformed into a state monopoly over formative instruction.

Necessary safeguards include plural schooling options, religious and philosophical educational alternatives, homeschooling or hybrid-schooling pathways where objective educational standards are met, curriculum transparency, parental notice, opt-out rights for contested non-core instruction, independent assessment options, judicial review, proportional accreditation standards, and a clear distinction between minimum competence and formative uniformity.

11. Epistemic Capture and Non-Neutral Expertise

Expertise may advise democratic judgment, but it must not replace democratic accountability.

Modern citizens are increasingly affected by international standards, expert frameworks, non-governmental organization (NGO) campaigns, foundation-funded research, technical standards, platform policies, health guidelines, AI ethics principles, financial compliance norms, educational standards, family-policy frameworks, and soft-law recommendations [29-32,40]. These instruments often appear neutral because they are written in the language of expertise, science, safety, health, sustainability, inclusion, or global responsibility.

The problem is not expert participation in policy formation. The problem arises when influence is presented as neutral expertise while funding sources, lobbying channels, stakeholder access, conflicts of interest, methodological assumptions, or political commitments remain opaque.

A recommendation is not neutral merely because it is written in technical language. Science may inform policy, but it must not become unaccountable rule.

Policy-capture and regulatory-capture literature explains how expertise, institutional incentives, funding structures, and technical language may redirect public decision-making away from transparent democratic accountability [29-32,40]. The Organisation for Economic Co-operation and Development (OECD) defines policy capture as a situation in which public decisions are consistently or repeatedly directed away from the public interest toward specific interests and recommends transparency, stakeholder engagement, accountability, and organizational integrity as safeguards [29]. Stigler's theory of economic regulation, Carpenter and Moss's work on regulatory capture, Lessig's account of institutional corruption, and Jasanoff's analysis of science advisers as policymakers all show that expertise and regulation must be examined institutionally rather than treated as automatically neutral [30-32,40].

Necessary safeguards include funding transparency, conflict-of-interest disclosure, lobbying registers, disclosure of meetings, methodological transparency, minority reports, independent replication, separation

between evidence and policy recommendation, democratic review before adopting international standards, public counter-hearings, and plural expert panels.

12. Physical Defensive Capacity and Weapons Law

This section does not treat firearms as the center of defensive sovereignty, but as one historically and legally contested subdomain of the broader question of lawful defensive capacity. The analysis is not jurisdiction-specific and does not assume that the same constitutional balance applies across legal systems. It is used here as a conceptual analogue, not as a universal policy prescription.

Weapons law is included because it offers a historical analogue for a wider problem examined throughout this paper: the tendency of governance systems to treat the citizen's defensive capacity itself as a risk source to be neutralized in advance. In earlier legal and political orders, this problem appeared most visibly in debates over physical defensive capacity, weapons possession, self-defense, and the state monopoly of force. In contemporary systems, the same structural logic increasingly appears in digital and infrastructural form. What physical disarmament has represented in some legal and political contexts, digital disarmament may represent in contemporary infrastructural settings: de-banking, de-platforming, algorithmic suppression, identity exclusion, communication shutdowns, and automated risk classification can all deprive citizens of the means to defend rights without formally abolishing those rights.

The point is not that firearms, bank accounts, platforms, encryption, and AI systems are identical. They are not. The point is that each concerns a defensive capacity: the ability to protect life, property, communication, reputation, livelihood, legal standing, and civic participation against unlawful or arbitrary power. Weapons law therefore serves as an analogue case within a broader theory of defensive sovereignty. It shows how the state may justify the reduction of citizen capacity by framing capacity itself as danger.

Weapons law is one expression of a deeper question: whether the citizen is recognized as a lawful defender of life, home, and property, or treated primarily as a risk source whose defensive capacity must be neutralized [59-64].

The argument does not deny the legitimacy of weapons regulation. Weapons can create real dangers, and the state may regulate them to prevent concrete harm, criminal misuse, negligence, unsafe storage, unlawful aggression, and access by violent or legally incompetent persons. The question is whether regulation targets concrete misuse or eliminates lawful defensive capacity as such [61-64].

The state often claims a monopoly over legitimate force, a point classically associated with Weber's account of the modern state [59]. Yet institutional protection may be delayed, retrospective, or unavailable at the moment of immediate danger. Police, courts, and criminal sanctions often intervene after harm has occurred. In such circumstances, citizens may remain responsible for survival, family protection, home, property, and risk while being deprived of meaningful immediate defensive capacity.

The section draws on the state monopoly of legitimate force, criminal-law theory, self-defense doctrine, and constitutional firearms jurisprudence while treating weapons law as only one subdomain of defensive sovereignty [59-64]. Blackstone's account of legal rights, Fletcher's criminal-law theory, Husak's critique of overcriminalization, and U.S. cases such as Heller and Bruen provide distinct reference points for the legal treatment of self-defense, weapons regulation, and defensive capacity [60-64].

Self-defense must be distinguished from vigilantism. Self-defense is immediate protection against unlawful aggression. Vigilantism is private punishment or coercive enforcement. Lawful possession must be distinguished from criminal misuse. Abstract dangerousness alone cannot justify blanket prohibition; it may justify proportionate, evidence-based regulation.

Necessary safeguards include lawful self-defense rights, proportionate weapons regulation, training and competence requirements, safe storage, exclusion of violent offenders, due process before confiscation or disarmament, appeal rights, protection against arbitrary confiscation, and clear distinction between defensive possession and criminal use.

13. Exit, Redundancy, Emergency Powers, and Non-Dismantlable Safeguards

13.1 Exit and Redundancy

Where there is no exit, permission becomes containment.

Citizens become vulnerable when every essential function is routed through a single infrastructure: one digital identity, one banking system, a small number of platforms, one app store, one payment network, one government portal, one AI-mediated access layer, one educational pathway, one family-recognition model, or one communications system. Where no alternative exists, denial of access becomes a form of containment [23-28,33-35,53-55].

Exit does not always mean physical departure. It may mean alternative channels: cash, analog public services, physical documents, offline emergency procedures, alternative platforms, open standards, interoperability, data portability, decentralized communication, encryption, independent media, independent courts, independent schools, alternative assessments, relational legal instruments, and protection against total smartphone or platform dependency.

This creates an unavoidable social trade-off. Redundant infrastructures such as cash, encryption, independent schooling, offline access, decentralized communication, or alternative payment channels can be misused. Cash may facilitate money laundering, encrypted communication may be used by criminals, and educational plurality may raise concerns about neglect or social isolation. But the existence of possible misuse does not justify destroying the infrastructure for all citizens. A free society must often tolerate the risk that protective spaces may be abused, because abolishing those spaces would make every citizen dependent on centralized permission. Misuse should be addressed through targeted, evidence-based, retrospective enforcement against concrete wrongdoing, not by preemptively dismantling the redundant systems that make ordinary freedom defensible.

Necessary safeguards include analog public access, cash availability, offline identity alternatives, public services without smartphone dependency, interoperable platforms, backup communication channels, decentralized infrastructure, data portability, plural educational pathways, relational legal tools, and prohibition of monopolistic control over civic access infrastructure.

13.2 Emergency Powers

The emergency becomes a sovereignty problem when temporary necessity hardens into permanent infrastructure.

Crises may justify extraordinary action. Terrorism, war, cyberattack, public disorder, financial crisis, health emergency, environmental disaster, educational disruption, or security threat may require temporary measures. The danger arises when temporary measures leave permanent legal, administrative, digital, educational, relational, or surveillance architecture behind [56-58].

Emergency-power theory shows that temporary necessity can produce permanent legal and administrative architecture unless constrained by review, sunset clauses, and rollback duties [56-58]. Emergency powers are especially prone to rights-disabling because they shift the burden of justification. Citizens may be asked to accept broad restrictions because the situation is urgent. Yet once emergency infrastructure exists, it may be repurposed, expanded, normalized, or preserved beyond the original crisis.

Temporary power becomes dangerous when it leaves permanent architecture behind.

Necessary safeguards include sunset clauses, parliamentary renewal, judicial review, burden of proof on the state, transparency duties, rollback duties after crisis, independent inquiry, prohibition of indefinite emergency tools, strict necessity, and proportionality.

14. The Resilient Sovereignty Safeguards Test

The Resilient Sovereignty Safeguards Test asks whether a right is protected not only in doctrine, but in operation.

1. Formal Right and Operational Capacity

Which right is formally protected? Which practical capacity makes the right usable?

2. Privacy, Harm, and Security Exception

Does a protected private sphere remain intact? Is there concrete harm to others, or only abstract risk rhetoric? Is the intervention targeted, lawful, evidence-based, reviewable, and proportionate?

3. Infrastructure and Dependency

Who controls the infrastructure necessary to exercise the right? Does the citizen depend on one authority, platform, bank, AI system, identity system, school system, family-status model, expert body, or regulatory channel?

4. Due Process and Contestability

Can the citizen obtain reasons, be heard, appeal, correct errors, and receive independent review?

5. Purpose Limitation and Emergency Control

Is the purpose narrowly limited? Can the measure expand beyond its original justification? Does it expire, or does it become permanent?

6. Anti-Capture and Transparency

Are funding, lobbying, algorithms, standards, curricula, family-policy assumptions, data sources, methods, and conflicts of interest transparent?

7. Exit, Redundancy, Education, Relationship, and Defensive Capacity

Are alternative channels available? Does the citizen retain lawful means to protect life, body, family, home, property, education, relationships, communication, and livelihood? Does the state require education only as minimum competence, or does it monopolize formative instruction by denying meaningful educational alternatives? Does the state protect lawful adult relational and caregiving arrangements, or does it make basic relational protection conditional on one approved family form?

The test does not invalidate all regulation. It identifies when regulation affects the operational conditions of rights and therefore requires a stronger burden of justification.

15. Synthesis: The Architecture of Defensive Sovereignty

The preceding analysis can be summarized as an architecture of defensive sovereignty.

Table 1. Operational Conditions, Disabling Mechanisms, and Resilient Safeguards

Domain	Formal Right	Operational Condition	Disabling Mechanism	Resilient Safeguard
Privacy	Private life	Confidentiality, home, encryption	Surveillance, generalized access	Warrants, purpose limitation, no backdoors
Family / Relationships	Private and family life	Legal recognition of caregiving, household, medical, inheritance, and property interests	Protection tied only to state-preferred family model	Contractual recognition, medical authorizations, inheritance tools, plural caregiving frameworks
Property	Ownership	Material independence	Expropriation, majority extraction	Compensation, judicial review
Speech	Expression	Reach and visibility	De-ranking, censorship, labeling	Appeal, transparency
Communication	Association	Internet and messaging	Shutdowns, platform blocking	Redundancy, VPN, court control
Finance	Economic participation	Banking and payment access	Debanking, freezing	Basic account, cash, appeal
AI	Fair treatment	Explanation and contestability	Automated exclusion	Human review, audits
Due Process	Remedy	Reasons and review	Administrative discretion	Independent courts, enforceable remedies
Education	Right to education / family life	Parental choice, plural schooling, neutral competence standards	Curricular monopoly, assessment capture, formative uniformity	Alternative pathways, curriculum transparency,

				opt-outs, independent assessment
Expertise	Public knowledge	Transparent evidence	Capture, pseudo-neutrality	conflict-of-interest disclosure, plural panels
Defense	Security	Lawful self-protection	Preventive neutralization of defensive capacity	Self-defense rights, proportionate regulation
Emergency	Public safety	Temporariness	Permanent infrastructure	Sunset clauses, rollback duties
Exit	Practical autonomy	Alternatives	Containment	Cash, analog access, interoperability

This architecture shows that rights depend on conditions. These conditions are not secondary technical details. They are the practical substance of citizenship. Citizens whose speech cannot be seen, whose money cannot be accessed, whose privacy cannot be protected, whose lawful relationships cannot be defended, whose property can be politically appropriated, whose children's education is monopolized, whose AI classification cannot be contested, whose expertise environment cannot be audited, whose communication can be shut down, and whose defensive capacity is wholly dependent on delayed institutional protection may possess rights in form while losing them in operation.

16. Conclusion: Rights Must Be Protected Against the Systems That Can Disable Them

This paper has argued that rights are secure only when citizens possess the practical, legal, material, financial, informational, technological, procedural, educational, relational, epistemic, and defensive means to use and defend them against arbitrary power.

The framework of defensive sovereignty extends the theory of conditionalized sovereignty by shifting attention from formal rights to operational conditions. It shows that modern rights may be disabled not only by direct prohibition, but also by infrastructural dependency, platform visibility control, financial exclusion, generalized surveillance, chilling effects, function creep, automated permission, educational monopoly, relational exclusion, hybrid power, epistemic capture, emergency normalization, and lack of exit.

The paper does not reject regulation, technology, education, family law, expertise, public safety, or democratic governance. It argues that these must remain constrained by due process, proportionality, transparency, contestability, purpose limitation, anti-capture safeguards, educational plurality, relational protection, and resilient alternatives.

The practical realization of resilient sovereignty safeguards requires more than abstract endorsement. It can proceed along at least three paths. Constitutionally, courts and constitutional interpreters may develop rights doctrine so that access to essential infrastructures--communication, payment systems, legal identity, educational plurality, due process, and meaningful appeal--is treated as part of the effective exercise of fundamental rights rather than as a merely administrative or commercial matter. Technologically, societies can support decentralized, encrypted, interoperable, and open-source protocols that resist monopolistic or centralized control by design. Regulatorily, lawmakers can draw a strict line between crime prevention

and politically or reputationally driven exclusion from public life, ensuring that tools built for fraud, terrorism, money laundering, or serious crime are not repurposed into mechanisms of civic neutralization. The final claim is therefore:

Free citizens are not merely persons to whom rights are declared. They are persons whose rights remain usable even when power finds those rights inconvenient.

Or, more directly:

Freedom becomes real only where rights cannot be silently disabled by the infrastructures that mediate modern life.

Conflict of Interest

The author declares no conflict of interest.

Acknowledgements

No external funding was received for this article. The author is solely responsible for the conception, analysis, writing, and final approval of the manuscript. Artificial intelligence (AI)-assisted tools were used for language editing, structural refinement, and readability improvement. The author reviewed, revised, and approved the final manuscript and takes full responsibility for its content.

References

1. Rubenstein, E. (2026). "Conditionalized Sovereignty: The Permission-Based Citizen and the Asymmetry of Legal Maturity." International Journal For Multidisciplinary Research, 8(3). https://doi.org/10.36948/ijfmr.2026.v08i03.79690
2. Pettit, P. (1997). Republicanism: A Theory of Freedom and Government. Oxford University Press.
3. Pettit, P. (2012). On the People's Terms: A Republican Theory and Model of Democracy. Cambridge University Press. https://doi.org/10.1017/CBO9781139017428
4. Lovett, F. (2022). "Republicanism." In E. N. Zalta and U. Nodelman (eds.), The Stanford Encyclopedia of Philosophy. Stanford University.
5. Skinner, Q. (1998). Liberty Before Liberalism. Cambridge University Press. https://doi.org/10.1017/CBO9781139197175
6. Mill, J. S. (1859). On Liberty. John W. Parker and Son.
7. Feinberg, J. (1984). Harm to Others: The Moral Limits of the Criminal Law. Oxford University Press. https://doi.org/10.1093/0195046641.001.0001
8. Feinberg, J. (1985). Offense to Others: The Moral Limits of the Criminal Law. Oxford University Press. https://doi.org/10.1093/0195052153.001.0001
9. Raz, J. (1979). "The Rule of Law and Its Virtue." In The Authority of Law. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198253457.003.0011
10. Fuller, L. L. (1964). The Morality of Law. Yale University Press.
11. Venice Commission. (2016). Rule of Law Checklist. Council of Europe.
12. Venice Commission. (2025). Updated Rule of Law Checklist. Council of Europe.
13. United Nations. (1966). International Covenant on Civil and Political Rights.

14. United Nations. (1948). Universal Declaration of Human Rights.
15. Council of Europe. (1950). European Convention on Human Rights.
16. European Court of Human Rights. (2024). Guide on Article 2 of Protocol No. 1 to the European Convention on Human Rights: Right to Education.
17. UN Human Rights Council. (2015). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Encryption, Anonymity and the Human Rights Framework, A/HRC/29/32.
18. Kaminski, M. E., & Witnov, S. (2015). "The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech." University of Richmond Law Review, 49, 465-521.
19. Bedi, S. (2021). "The Myth of the Chilling Effect." Harvard Journal of Law & Technology, 35(1), 267-307.
20. Solove, D. J. (2008). Understanding Privacy. Harvard University Press.
21. Cohen, J. E. (2012). Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. Yale University Press. https://doi.org/10.12987/9780300177930
22. European Court of Human Rights. (2024). Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence.
23. Access Now and #KeepItOn. (2025). Emboldened Offenders, Endangered Communities: Internet Shutdowns in 2024. Access Now.
24. Access Now and #KeepItOn. (2026). Rising Repression Meets Global Resistance: Internet Shutdowns in 2025. Access Now.
25. Gillespie, T. (2018). Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. Yale University Press. https://doi.org/10.12987/9780300235029
26. Klonick, K. (2018). "The New Governors: The People, Rules, and Processes Governing Online Speech." Harvard Law Review, 131, 1598-1670.
27. United Nations. (2011). Guiding Principles on Business and Human Rights. United Nations.
28. Ruggie, J. G. (2013). Just Business: Multinational Corporations and Human Rights. Norton.
29. OECD. (2017). Preventing Policy Capture: Integrity in Public Decision Making. OECD Publishing. https://doi.org/10.1787/9789264065239-en
30. Stigler, G. J. (1971). "The Theory of Economic Regulation." Bell Journal of Economics and Management Science, 2(1), 3-21. https://doi.org/10.2307/3003160
31. Carpenter, D., & Moss, D. A. (eds.). (2014). Preventing Regulatory Capture: Special Interest Influence and How to Limit It. Cambridge University Press. https://doi.org/10.1017/CBO9781139565875
32. Lessig, L. (2011). Republic, Lost: How Money Corrupts Congress--and a Plan to Stop It. Twelve.
33. European Parliament and Council. (2024). Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence. Official Journal of the European Union.
34. National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework 1.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1
35. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. UNESCO.
36. Citron, D. K. (2008). "Technological Due Process." Washington University Law Review, 85, 1249-1313.

37. Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press.
38. Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). "Fairness and Abstraction in Sociotechnical Systems." In Proceedings of the Conference on Fairness, Accountability, and Transparency, 59-68. Association for Computing Machinery. https://doi.org/10.1145/3287560.3287598
39. Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and Machine Learning. fairmlbook.org.
40. Jasanoff, S. (1990). The Fifth Branch: Science Advisers as Policymakers. Harvard University Press.
41. Meyer v. Nebraska, 262 U.S. 390 (1923).
42. Pierce v. Society of Sisters, 268 U.S. 510 (1925).
43. Wisconsin v. Yoder, 406 U.S. 205 (1972).
44. Konrad v. Germany, European Court of Human Rights, Application No. 35504/03.
45. Obergefell v. Hodges, 576 U.S. 644 (2015).
46. Lawrence v. Texas, 539 U.S. 558 (2003).
47. Oliari and Others v. Italy, European Court of Human Rights, Applications Nos. 18766/11 and 36030/11.
48. Schalk and Kopf v. Austria, European Court of Human Rights, Application No. 30141/04.
49. Vallianatos and Others v. Greece, European Court of Human Rights, Applications Nos. 29381/09 and 32684/09.
50. Waldron, J. (1988). The Right to Private Property. Clarendon Press.
51. Honoré, A. M. (1961). "Ownership." In A. G. Guest (ed.), Oxford Essays in Jurisprudence. Oxford University Press.
52. Hohfeld, W. N. (1913). "Some Fundamental Legal Conceptions as Applied in Judicial Reasoning." Yale Law Journal, 23(1), 16-59. https://doi.org/10.2307/785533
53. European Parliament and Council. (2014). Directive 2014/92/EU on the Comparability of Fees Related to Payment Accounts, Payment Account Switching and Access to Payment Accounts with Basic Features. Official Journal of the European Union.
54. Demirgüç-Kunt, A., Klapper, L., Singer, D., & Ansar, S. (2022). The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. World Bank. https://doi.org/10.1596/978-1-4648-1897-4
55. de Goede, M. (2012). Speculative Security: The Politics of Pursuing Terrorist Monies. University of Minnesota Press.
56. Gross, O., & Ní Aoláin, F. (2006). Law in Times of Crisis: Emergency Powers in Theory and Practice. Cambridge University Press.
57. Dyzenhaus, D. (2006). The Constitution of Law: Legality in a Time of Emergency. Cambridge University Press.
58. Ferejohn, J., & Pasquino, P. (2004). "The Law of the Exception: A Typology of Emergency Powers." International Journal of Constitutional Law, 2(2), 210-239. https://doi.org/10.1093/icon/2.2.210
59. Weber, M. (1946). "Politics as a Vocation." In H. H. Gerth and C. Wright Mills (eds.), From Max Weber: Essays in Sociology. Oxford University Press.
60. Blackstone, W. (1765-1769). Commentaries on the Laws of England. Clarendon Press.
61. Fletcher, G. P. (1998). Basic Concepts of Criminal Law. Oxford University Press.

62. Husak, D. (2008). Overcriminalization: The Limits of the Criminal Law. Oxford University Press.
63. District of Columbia v. Heller, 554 U.S. 570 (2008).
64. New York State Rifle & Pistol Association, Inc. v. Bruen, 597 U.S. 1 (2022).