ARTICLE

DELEGATED DIGITAL POWER AND THE SEPARATION OF POWERS: A COMPARATIVE STUDY OF NIGERIA AND CANADA

Dr. Emmanuel Ojotu*

Abstract

Digital transformation has changed how public power is distributed among the institutions of government. Legislatures increasingly enact framework statutes that delegate substantial rule-making, investigative and enforcement authority to ministers, regulators and specialised agencies. This raises the research problem addressed in this article: how much law-making power may be transferred from the legislature to executive and regulatory bodies in the digital field without undermining the separation of powers and constitutional accountability? The article has three objectives: to identify the risks that the lengthening regulatory chain of the digital state poses to the separation of powers; to compare how two federations with different constitutional structures, presidential Nigeria and parliamentary Canada, manage those risks; and to propose a framework for assessing delegated digital power in both. Methodologically, it combines doctrinal analysis of constitutional provisions, statutes, regulations and case law with a functional comparative method. It examines the Nigeria Data Protection Act 2023 and the Nigeria Data Protection Commission, the 2022 platform Code of Practice of the National Information Technology Development Agency, the suspension of Twitter in 2021, and Canada's telecommunications, privacy and broadcasting regimes, including its cyber security legislation, which received Royal Assent in June 2026. The article argues that digital regulation does not eliminate the separation of powers but changes its institutional expression. It finds that Nigeria's formal separation of legislative and executive power has not prevented rights-sensitive digital rules from being made by executive action and agency codes, while Canada's acceptance of broad delegation is tempered by prepublication, parliamentary scrutiny and reasonableness review. It proposes an authority–standards–accountability framework and a model of 'bounded digital delegation' that distinguishes technical from normative discretion.

Keywords – Separation of powers; delegated legislation; digital regulation; data protection; cyber security; platform regulation; Nigeria; Canada

I. INTRODUCTION

The separation of powers is commonly understood as a structural principle requiring governmental power to be distributed among legislative, executive and judicial institutions. Digital governance

*PhD, LLM, LLB, BL, BA Phil. Sessional Instructor in Constitutional Law, Faculty of Law, University of Windsor, Canada. Director, Ojotu Law Firm, Ontario, Canada.

complicates this model. Modern digital legislation typically sets out broad statutory objectives and leaves the detail to ministers, regulators and specialised agencies. The reasons are understandable. Technology develops faster than legislation can be amended, and no legislature can realistically prescribe every technical requirement governing data processing, cyber security, platform moderation or artificial intelligence.

Flexibility, however, produces a constitutional difficulty. When a regulator is authorised to make binding rules, investigate breaches of those rules and impose penalties, it exercises functions resembling legislation, administration and adjudication at the same time. Digital regulation therefore poses a question that is old in form but new in scale: how can the state obtain the regulatory flexibility that rapidly changing technologies require without allowing executive and regulatory institutions to accumulate excessive law-making power?

The question is especially useful in comparing Nigeria and Canada, because the two federations approach the separation of powers from different constitutional starting points. Nigeria's Constitution vests the legislative powers of the Federation in the National Assembly and the executive powers in the President, in separate provisions, within a presidential system.[1] Canada's Constitution divides legislative authority between Parliament and the provincial legislatures, but within each order of government the executive is drawn from and responsible to the legislature under the conventions of responsible government.[2] The Supreme Court of Canada has said that the Canadian Constitution 'does not insist on a strict separation of powers'.[3] The concept cannot therefore simply be transplanted from one jurisdiction to the other.

For that reason, this article uses a functional conception. The separation of powers in digital governance concerns the distribution, limitation and accountability of law-making, implementation and adjudicative authority among institutions, whatever the formal relationship between legislature and executive. On that conception, the central question in both countries is the same: whether the legislature has retained responsibility for the basic normative choices in digital regulation, and whether the authority it has delegated remains subject to effective control.

Section II describes the 'lengthening regulatory chain' of the digital state and the risks it creates. Sections III and IV examine Nigeria and Canada. Section V develops a comparative framework built on authority, standards and accountability, and section VI distinguishes technical

[1] CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA (1999), §§ 4(1), 5(1).
[2] Constitution Act, 1867, 30 & 31 Vict., c. 3, §§ 9, 17, 91–92 (U.K.).
[3] *Reference re Secession of Quebec*, [1998] 2 S.C.R. 217, ¶ 15 (Can.).

from normative discretion. Section VII sets out the model of bounded digital delegation, and section VIII concludes.

II. THE SEPARATION OF POWERS IN THE DIGITAL STATE

Traditional legislation follows a relatively simple sequence: the legislature enacts a statute, the executive implements it, and the courts review its application. Digital governance increasingly follows a longer chain. The legislature enacts a framework statute; a minister or regulator makes regulations; the regulator issues directives, codes or technical standards; compliance orders and administrative penalties follow; and judicial review comes last, if at all. Each link in the chain involves a choice about the content of the law, and each is further from the legislature that is the source of democratic authority.

The lengthening chain produces three risks.

The first is *legislative displacement*. The legislature may enact statutory language so broad that the substantive content of the law is effectively determined by the executive. The legislature retains formal authority but surrenders its practical role as the forum in which basic normative choices are made.

The second is *executive accumulation*. A single regulator may hold rule-making, investigative and enforcement powers at once, and in some cases adjudicative powers as well. Such combinations are common in modern administration and are not unlawful in themselves.[4] But they concentrate in one body the functions that the separation of powers traditionally divides, and they make the internal design of the regulator, rather than the relationship between branches, the principal safeguard.

The third is *judicial compression*. Courts usually review administrative decisions only after regulatory power has been exercised, often after rules have shaped the conduct of an entire industry. Where the rules themselves are framed as non-binding guidance, codes or confidential directions, review may be difficult to obtain at all.

None of these risks means that delegation is unconstitutional. Delegation is an ordinary and necessary feature of modern government. The constitutional question is one of limits and accountability.

[4]EOIN CAROLAN, THE NEW SEPARATION OF POWERS: A THEORY FOR THE MODERN STATE (2009).

III. NIGERIA

a. Constitutional architecture

Nigeria's Constitution provides a strong textual foundation for analysing delegation. The legislative powers of the Federation are vested in the National Assembly,[5] and the executive powers of the Federation extend to 'the execution and maintenance of this Constitution, all laws made by the National Assembly and to all matters with respect to which the National Assembly has, for the time being, power to make laws'.[6] Judicial powers are vested in the courts.[7] Nigerian law has long accepted that the National Assembly may authorise the executive and statutory bodies to make subsidiary legislation, which the Interpretation Act defines to include orders, rules, regulations and other instruments made under an Act.[8] There is, however, no general statute governing the making, publication and parliamentary scrutiny of subsidiary legislation comparable to Canada's Statutory Instruments Act. Control of delegated legislation therefore rests on the enabling statute in each case and on judicial review for vires.

The Supreme Court's decision on Executive Order 10 illustrates the constitutional boundary. In 2022 the Court held that the President could not, by executive order, direct the deduction of funds for state legislatures and judiciaries from state allocations, because doing so amounted to legislating without constitutional authority.[9] The case did not concern digital regulation. Its principle, however, applies directly to it: executive and regulatory instruments must be anchored in constitutional or statutory authority, and the executive may not supply by directive what the legislature has not enacted.

Nigeria's experience also shows the dangers of digital power exercised without statutory authority. In June 2021 the federal government suspended the operation of Twitter in Nigeria, after the platform removed a post by the President, by announcement of the Minister of Information. The suspension lasted until January 2022. In July 2022 the ECOWAS Court of Justice held that the suspension violated the right to freedom of expression under the African Charter on Human and Peoples' Rights, principally because the government could identify no law authorising it.[10] The

[5] CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA (1999), § 4(1)–(2).
[6] *Id.* § 5(1)(b).
[7] *Id.* § 6.
[8] Interpretation Act, Cap. (I23), § 18(1), Laws of the Federation of Nigeria (2004).
[9] *Att'y Gen. of Abia State v. Att'y Gen. of the Fed'n*, SC/CV/655/2020 (Feb. 11, 2022) (S.C.) (Nigeria).
[10] *Socio-Econ. Rts. & Accountability Project (SERAP) v. Fed. Republic of Nigeria*, Judgment No. ECW/CCJ/JUD/40/22 (ECOWAS Ct. Just. July 14, 2022).

episode is an extreme example of the separation of powers problem in digital governance: a significant restriction on communication imposed by executive announcement, without legislative authority and without prior judicial control.

b. The Nigeria Data Protection Commission

The Nigeria Data Protection Act 2023, signed into law in June 2023, provides the most important case study. It established the Nigeria Data Protection Commission, replacing a regime that had rested on the Nigeria Data Protection Regulation 2019, a regulation issued by the National Information Technology Development Agency (NITDA) under its general statutory powers.[11] That earlier arrangement was itself striking from a separation of powers perspective. For four years Nigeria's principal data protection rules were made by an executive agency rather than enacted by the legislature. The Court of Appeal nonetheless treated the Regulation as an instrument giving effect to the constitutional right to privacy in section 37 of the Constitution, which it held to include the protection of personal data.[12]

The 2023 Act put data protection on a statutory footing, but it delegated extensive power to the Commission. The Commission's functions include regulating the deployment of technological and organisational measures to secure personal data and registering data controllers and processors 'of major importance'.[13] Its powers include overseeing implementation of the Act, issuing 'regulations, rules, directives and guidance', investigating violations and imposing penalties.[14] The Act declares that the Commission 'shall be independent in the performance of its functions'.[15] It may receive complaints and investigate on its own initiative, issue compliance orders and make enforcement orders imposing penalties. For data controllers of major importance, those penalties may reach the greater of ten million naira or two per cent of annual gross revenue.[16] A person aggrieved by an order may apply for judicial review within thirty days.[17] In March 2025 the Commission issued a General Application and Implementation Directive that elaborates many of the Act's obligations in considerable detail.

---

[11] Nigeria Data Protection Regulation (2019) (issued under the National Information Technology Development Agency Act, 2007, § 6) (Nigeria).

[12] *Inc. Trs. of Digit. Rts. Laws. Initiative v. Nat'l Identity Mgmt. Comm'n*, (2021) LPELR-55623 (CA), Appeal No. CA/IB/291/2020 (Sept. 24, 2021) (Nigeria).

[13] Nigeria Data Protection Act, 2023, § 5 (Nigeria).

[14] *Id.* § 6(c).

[15] *Id.* § 7.

[16] *Id.* §§ 46–48.

[17] *Id.* § 50.

The Commission thus combines rule-making, investigation and sanction in a single body. That concentration is not unlawful; specialised regulators frequently combine functions, and the Act's provision for judicial review supplies an external check. But the concentration raises a question of structural accountability. Several features of the Act mitigate it: the statute sets out the principles of lawful processing, the bases of processing and the rights of data subjects in some detail, so that the Commission's rule-making operates within relatively clear legislative standards. Others aggravate it. The statute does not require the Commission to consult publicly before issuing regulations or directives, does not provide for the legislature to scrutinise them, and does not separate the officers who investigate from those who decide on penalties. The more significant the regulatory power, the more important it becomes that the enabling statute provide clear standards and procedures. The Nigeria Data Protection Act does well on the first and less well on the second.

c. Platform regulation by code

NITDA's Code of Practice for Interactive Computer Service Platforms and Internet Intermediaries, issued in 2022 shortly after the end of the Twitter suspension, provides a second example. The Code requires large platforms to register in Nigeria, appoint a local representative, act on notices of unlawful content within specified periods and take measures against disinformation, and it reserves to NITDA the power to review and amend it.[18] Vincent Obia has described the Code as a 'radical co-regulatory turn', which shifts regulatory attention from individual users to duties of care imposed on platforms.[19]

The regulatory significance of such a code is considerable. A code issued by an administrative agency can shape the legal environment in which global technology companies operate and, through them, the speech of millions of users. Yet its legal basis lies in general statutory functions rather than in a specific legislative mandate to regulate online content, and its content was never debated by the National Assembly. When obligations of this kind, which bear directly on freedom of expression, are developed through executive codes, the separation of powers concern is acute. The legislature has not made the basic normative choices about what speech may be restricted and how. An agency whose primary mandate is technological development has made them.

[18]Nat'l Info. Tech. Dev. Agency, Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries (2022).

[19]Vincent Obia, *Digital Policy and Nigeria's Platform Code of Practice: Towards a Radical Co-Regulatory Turn*, 7 Data & Pol'y e12 (2025).

IV. CANADA

a. Delegation in a parliamentary system

Canada presents a different constitutional structure. Because the federal executive is responsible to Parliament, the separation of powers in Canada does not require the institutional separation characteristic of a presidential system. Canadian law has always permitted broad delegations of law-making power. As early as 1918 the Supreme Court upheld the wartime delegation of virtually unlimited regulatory power to the Governor in Council,[20] and it has since upheld broad delegations in peacetime. In the *Greenhouse Gas Pollution Pricing Act References*, it upheld a 'Henry VIII' clause permitting the executive to amend the statute's schedule of covered provinces, reasoning that Parliament retains the power to revoke the delegation and that the executive's power remained bounded by the statute's purposes.[21] Canadian constitutional law contains no non-delegation doctrine of the American kind; the only firm limit is that Parliament may not abdicate its legislative role altogether.

The principal controls on delegated legislation in Canada are therefore procedural and administrative rather than constitutional. The Statutory Instruments Act requires regulations to be examined for legality, registered and published.[22] The Standing Joint Committee for the Scrutiny of Regulations reviews regulations for consistency with their enabling statutes. The federal regulatory policy generally requires prepublication in the *Canada Gazette* and public comment before significant regulations are made. And since 2024 the Supreme Court has made clear that regulations are reviewable for reasonableness under the general framework of administrative law. Their validity depends on whether they are consistent with the text, context and purpose of the enabling statute, rather than on a strong presumption of validity.[23] That development strengthens judicial control of delegated rule-making, including in digital regulation.

b. Independent regulators and political direction

Canadian digital regulation also illustrates a distinctive feature of the parliamentary model: the coexistence of independent regulators with executive powers of direction. The Canadian Radio-television and Telecommunications Commission regulates broadcasting and telecommunications at

[20] *In re Gray*, (1918) 57 S.C.R. 150 (Can.).
[21] *References re Greenhouse Gas Pollution Pricing Act*, 2021 SCC 11, [2021] 1 S.C.R. 175 (Can.).
[22] Statutory Instruments Act, R.S.C. 1985, c. S-22, §§ 3–11 (Can.).
[23] *Auer v. Auer*, 2024 SCC 36 (Can.); *TransAlta Generation P'ship v. Alberta (Minister of Agric. & Forestry)*, 2024 SCC 37 (Can.).

arm's length, but the Governor in Council may issue policy directions to it and may vary or rescind its decisions.[24] The Online Streaming Act extended the Commission's broadcasting jurisdiction to online platforms, leaving much of the detail to the Commission under a policy direction from the Governor in Council.[25] The Supreme Court has policed the limits of such regimes, holding that the Commission exceeded its statutory authority when it made an order concerning the broadcast of Super Bowl advertisements.[26] The courts thus police both the delegation from Parliament to the regulator and the regulator's compliance with the limits of its mandate.

Data protection offers an instructive contrast with Nigeria. Under the Personal Information Protection and Electronic Documents Act, the federal Privacy Commissioner investigates complaints and makes findings, but has no power to issue binding orders or impose penalties. Enforcement requires an application to the Federal Court, which hears the matter afresh.[27] Parliament's attempts to give the Commissioner order-making powers, and to create a separate Personal Information and Data Protection Tribunal to impose penalties, lapsed when Parliament was prorogued in January 2025. Whatever its practical weaknesses, the Canadian model separates investigation from adjudication in a way that the Nigerian model does not.

c. The 2026 cyber security legislation

Canada's cyber security legislation, which received Royal Assent on 16 June 2026, provides a particularly important contemporary example of delegated digital power.[28] Its first Part amends the Telecommunications Act to add the promotion of the security of the Canadian telecommunications system to the statute's objectives. It authorises the Governor in Council and the Minister of Industry to make orders directing telecommunications service providers to do, or refrain from doing, anything necessary to secure the system. Such orders may include prohibiting the use of products or services from specified suppliers. These amendments came into force on Royal Assent. The second Part enacts the Critical Cyber Systems Protection Act, which allows the Governor in Council to designate operators of critical cyber systems in vital federally regulated sectors, including telecommunications, energy transmission, nuclear energy, transportation, banking, and clearing and

[24]Telecommunications Act, S.C. 1993, c. 38, §§ 8, 12 (Can.).
[25]Online Streaming Act, S.C. 2023, c. 8 (Can.).
[26]*Bell Canada v. Canada (Att'y Gen.)*, 2019 SCC 66, [2019] 4 S.C.R. 845 (Can.).
[27]Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, §§ 11–16 (Can.); *see, e.g.*, *Canada (Privacy Comm'r) v. Facebook, Inc.*, 2024 FCA 140 (Can.).
[28]An Act Respecting Cyber Security, Amending the Telecommunications Act and Making Consequential Amendments to Other Acts, S.C. 2026 (Bill C-8, 45th Parl., 1st Sess.) (Can.) (assented to June 16, 2026).

settlement. Designated operators must establish cyber security programmes, mitigate supply-chain risks and report incidents, and the Governor in Council may issue binding cyber security directions to them.

The legislation represents a significant transfer of regulatory detail from Parliament to the executive. The vital services and systems, the classes of operators, the content of security programmes and the directions themselves are all determined by the executive. The orders and directions may be kept confidential, and penalties for non-compliance are substantial. At the same time, the statute provides for judicial review of orders and directions, with special procedures for the protection of sensitive information. Those procedures permit the court to receive evidence in the absence of the applicant, which critics have noted is not accompanied by the special advocates available in immigration security proceedings.

The combination is constitutionally significant. It reflects a model in which Parliament creates the regulatory architecture while the executive supplies technical and operational detail, subject to judicial oversight. The legislation's predecessor bill, introduced in 2022, had been criticised for the breadth of its delegations and the secrecy of its orders, and lapsed when Parliament was prorogued. Whether the final scheme adequately bounds executive power will depend on the regulations made under it and on how the courts approach review of confidential security orders.

V. A COMPARATIVE FRAMEWORK: AUTHORITY, STANDARDS AND ACCOUNTABILITY

The comparison reveals three dimensions along which delegated digital power can be assessed, regardless of whether the constitutional system is presidential or parliamentary.

The first is *authority*. Has the legislature clearly authorised the regulator or minister to act in the relevant field? The Twitter suspension in Nigeria failed this test at its most basic level, because no statute authorised it. NITDA's platform Code raises a subtler question of authority. A general statutory mandate to develop information technology arguably does not authorise the regulation of online speech. By contrast, the Nigeria Data Protection Act and Canada's cyber security legislation each contain express grants of authority for the regulatory powers they confer.

The second is *standards*. Has the legislature established meaningful standards that guide and confine the exercise of delegated power? The Nigeria Data Protection Act scores relatively well, because it sets out the principles and bases of lawful processing and the rights of data subjects in the

statute. The Canadian cyber security legislation is weaker on this dimension. Its central standard, that orders be 'necessary' to secure the telecommunications system or protect critical cyber systems, leaves the executive considerable latitude, although it is tied to an identifiable statutory purpose.

The third is *accountability*. Can those affected challenge the exercise of delegated power before independent institutions, and is the power subject to political scrutiny? Here the two systems differ markedly. Canada combines prepublication, parliamentary scrutiny of regulations and reasonableness review of regulations themselves. Nigeria relies principally on judicial review after the fact, with no general requirement of consultation or legislative scrutiny.

These dimensions can be summarised as an *authority–standards–accountability* framework. It provides a common analytical vocabulary for systems with different constitutional structures, because it asks about the relationship between delegated power and its sources of control rather than about the formal separation of branches.

VI. TECHNICAL DISCRETION AND NORMATIVE DISCRETION

Digital technology provides an unusually strong justification for delegation. Technical standards may need to change rapidly in response to new threats or capabilities. A statute cannot easily specify cyber security protocols, encryption standards, data security controls, incident-reporting procedures or algorithmic risk classifications, and if it did, the specification would soon be obsolete. Delegation is therefore functionally necessary.

But technological complexity should not become a constitutional blank cheque. A regulator's technical expertise may justify technical discretion; it does not necessarily justify unlimited normative discretion. The distinction is central to this article.

Technical discretion is the power to determine how a statutory requirement should be implemented in light of technical circumstances. A regulator that decides which encryption standard satisfies a statutory duty to protect personal data, or which security controls are appropriate for a particular class of critical infrastructure, exercises technical discretion. The legislature has made the normative choice that data must be secured or infrastructure protected, and the regulator applies expertise to determine how.

Normative discretion is the power to determine what conduct should be legally required, permitted or prohibited in the first place. A regulator that decides which categories of online speech platforms must remove, or that creates a new restriction on communication without clear legislative

authority, exercises normative discretion. The choice is one of value rather than technique, and it is the kind of choice that the separation of powers reserves to the legislature.

The first kind of discretion is readily justified by expertise. The second raises a much stronger separation of powers concern, because expertise provides no special claim to make value choices on behalf of the political community. The distinction is not always sharp. A choice about how quickly platforms must remove content is technical in form but normative in effect, because it shapes how much lawful speech will be removed in error. But the distinction provides a useful guide to the intensity of the safeguards that delegation requires. The more normative the delegated discretion, the more specific the legislative standards and the more robust the procedural and judicial safeguards should be.

Applied to the examples examined here, the distinction suggests that Canada's cyber security orders are largely, though not entirely, exercises of technical discretion. Their potential effects on competition, privacy and the availability of services, however, give them a normative dimension that warrants careful review. The Nigeria Data Protection Commission's directives are primarily technical, because the Act makes the main normative choices. NITDA's platform Code, which determines what content must be removed and how quickly, involves substantial normative discretion exercised without specific legislative authority. That is where the separation of powers concern is greatest.

VII. BOUNDED DIGITAL DELEGATION

This article proposes a model of *bounded digital delegation*, consisting of six safeguards. The model does not seek to prevent delegation, which digital regulation requires. It seeks to ensure that delegated power remains connected to legislative authority and subject to effective control.

Clear enabling authority. The statute should identify the subject matter and purpose of the delegated power. General mandates to promote or develop technology should not be read as authority to regulate rights-sensitive matters such as speech or surveillance.

Substantive limits. Delegated authority should be confined by meaningful legislative standards, with greater specificity where the discretion is normative rather than technical. The legislature should make the basic choices about which rights may be limited, for what purposes and to what extent.

Procedural safeguards. Major digital rules should ordinarily be subject to public consultation, publication and reasoned decision-making. Canada's practice of prepublication provides a model. Nigeria's digital regulators would benefit from a statutory duty to consult before issuing binding regulations, codes and directives.

Institutional separation. Where feasible, rule-making, investigation and adjudication within a single regulator should be subject to internal safeguards against conflicts of interest, such as the separation of investigating and decision-making officers or, for the most serious penalties, adjudication by a separate tribunal or court.

Transparency. Regulatory codes, directives and enforcement policies should be publicly accessible. Where confidentiality is genuinely necessary, as with some cyber security directions, the legislature should require periodic reporting to Parliament or to a security-cleared committee so that the overall use of the power can be scrutinised.

Judicial review. Courts must remain able to review whether digital regulators and ministers have acted within their statutory authority and constitutional limits. Where sensitive information is involved, the procedures for review should include safeguards, such as special advocates, that preserve the fairness of the proceedings.

The two systems require different emphases. In Nigeria, the priority is to strengthen the connection between digital regulation and legislative authority. That means giving specific statutory bases to rights-sensitive regimes such as platform regulation, adopting general procedural rules for the making and publication of subsidiary legislation, and building institutional separation into the enforcement processes of powerful regulators such as the Data Protection Commission. In Canada, where the legislative framework for delegation is more developed, the priority lies with the standards and safeguards attached to executive security powers, and with the continued development of reasonableness review of regulations after *Auer*.

VIII. CONCLUSION

Digital law has made delegated power more necessary than ever. It has also made the constitutional control of delegated power more difficult. Nigeria and Canada demonstrate two different institutional responses. Nigeria's presidential structure places particular emphasis on the formal distribution of authority between legislature and executive, but its digital governance has at times been conducted through executive action and agency codes with uncertain statutory

foundations. Canada's parliamentary system accepts broad delegation as a matter of constitutional principle, but surrounds it with procedural requirements, parliamentary scrutiny and increasingly searching judicial review.

In both systems, however, the central constitutional question is the same: how much digital law may be made outside the legislature before delegation becomes institutional displacement? The answer proposed here is bounded digital delegation. The legislature must establish the legal authority, the substantive standards and the institutional framework, and must itself make the normative choices that digital regulation involves. Regulators may supply technical detail and implement the legislative scheme. Courts must remain available to police the boundaries. Digital transformation should change the methods of regulation. It should not displace the constitutional principle that public power requires legal authority and institutional accountability.