

TÜRKİYE'S TRIPARTITE DIGITAL REGULATION: A KANTIAN DEONTOLOGICAL ANALYSIS OF PDPL, LAW NO. 5651, AND LAW NO. 4054*

*Türkiye'nin Üçlü Dijital Düzenlemesi:
KVKK, 5651 Sayılı Kanun ve 4054 Sayılı Kanun'un Kantçı Deontolojik Analizi*

Nasir QADRI**

L&JR

Year: 17, Issue: 32

July 2026

pp.115-142

Article Information

Submitted : 13.5.2026

*Revision
Requested* : 3.6.2026

*Last Version
Received* : 14.6.2026

Accepted : 17.7.2026

Article Type

Research Article

Abstract

Türkiye presents itself as a GDPR-aligned digital governance actor, yet simultaneously operates three legally inconsistent instruments: the Law on Protection of Personal Data (PDPL), which partially mirrors EU data protection standards; Law No. 5651, which authorises administrative platform blocking without prior judicial authorisation and criminalises broadly defined online expression; and the draft amendment to Competition Law No. 4054, which adopts Digital Markets Act gatekeeper thresholds while remaining silent on individual rights. No existing scholarship has analysed these three instruments together through a unified ethical framework. This article applies Kantian deontological theory, specifically the categorical imperative and the principle of treating persons as ends in themselves, to evaluate the internal coherence of Türkiye's tripartite digital regulatory framework. It argues that the PDPL partially honours deontological principles, Law No. 5651 structurally violates them, and the draft amendment to Law No. 4054 is deontologically silent in ways that compound the contradiction. This tripartite inconsistency, the article concludes, provides a structural explanation for Türkiye's continued failure to obtain EU adequacy recognition, and resolving it requires targeted legislative reforms to each instrument grounded in deontological principles. The findings contribute an original analytical framework for identifying jurisdictional contradictions

* There is no requirement of Ethics Committee Approval for this study.

** Phd Student Public International Law Koc University, İstanbul/Türkiye,
e-mail: Nqadri25@ku.edu.tr, <https://orcid.org/0000-0002-5670-7115>

in GDPR-adjacent digital regulatory regimes and offer three concrete reform recommendations for Turkish digital governance.

Keywords: Digital Regulation; Kantian Deontology, Personal Data Protection, Internet Censorship, EU Adequacy Decision, Gatekeeper Regulation, Turkish Digital Law, PDPL

Özet

Türkiye, GDPR ile uyumlu bir dijital yönetim aktörü olarak sunulmakta; ancak aynı anda üç hukuki bakımdan tutarsız araç işletmektedir: AB veri koruma standartlarını kısmen yansıtan Kişisel Verilerin Korunması Kanunu (KVKK); önceden yargısal denetim olmaksızın idari platform engelleme yetkisi tanıyan ve geniş kapsamlı çevrimiçi ifadeyi suç olarak tanımlayan 5651 Sayılı Kanun; ve bireysel haklar konusunda sessiz kalırken Dijital Piyasalar Yasası'nın kapı bekçisi eşiklerini benimseyen 4054 Sayılı Rekabetin Korunması Hakkında Kanun'un taslak değişikliği. Mevcut literatürde bu üç araç, bütünleşik bir etik çerçeve aracılığıyla birlikte hiç analiz edilmemiştir. Bu makale, Türkiye'nin üçlü dijital düzenleyici çerçevesinin iç tutarlılığını değerlendirmek amacıyla Kantçı deontolojik teoriyi, özellikle kategorik buyruğu ve kişilere her zaman amaç olarak davranılması ilkesini uygulamaktadır. KVKK'nın deontolojik ilkeleri kısmen karşıladığı, 5651 Sayılı Kanun'un bu ilkeleri yapısal olarak ihlal ettiği ve 4054 Sayılı Kanun taslak değişikliğinin çelişkiyi derinleştiren biçimde deontolojik açıdan sessiz kaldığı savunulmaktadır. Bu üçlü tutarsızlığın, Türkiye'nin AB yeterlilik kararı alamamasının yapısal bir açıklamasını oluşturduğu ve çözümünün her bir araca yönelik deontolojik ilkelere dayalı hedefli yasal reformlar gerektirdiği sonucuna varılmaktadır. Bulgular, GDPR ile uyumlu dijital düzenleyici rejimlerdeki yetki alanı çelişkilerini tespit etmeye yönelik özgün bir analitik çerçeve sunmakta ve Türk dijital yönetimi için üç somut reform önerisi getirmektedir.

Anahtar Kelimeler: Dijital Düzenleme, Kantçı Deontoloji, Kişisel Verilerin Korunması, İnternet Sansürü, AB Yeterlilik Kararı, Kapı Bekçisi Düzenlemesi, Türk Dijital Hukuku, KVKK

INTRODUCTION

On 6 February 2023, as rescue teams scrambled to locate survivors of the earthquakes that devastated southern Türkiye and claimed more than 50,000 lives, the Turkish government restricted access to Twitter, the platform that citizens were using to coordinate emergency assistance and communicate their locations to rescuers.¹ The restriction was imposed under Article 8A of Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes

¹ Freedom House, *Freedom on the Net 2024: Türkiye Country Report* (Freedom House 2024) <https://freedomhouse.org/country/Türkiye/freedom-net/2024> accessed 1 May 2026.

Committed Through Such Publications, which authorises the Information and Communication Technologies Authority (BTK) to issue access-blocking orders without prior judicial authorisation.² The episode lasted eight hours, with its consequences, in terms of delayed rescue coordination, remaining disputed; its constitutional and ethical implications do not. A state that simultaneously enacts legislation promising to protect the personal data and communicative autonomy of its citizens, while retaining unreviewable administrative power to silence the platforms through which that autonomy is exercised, has not resolved a regulatory tension, but rather institutionalised one.

This article argues that Türkiye's digital regulatory framework contains a tripartite internal contradiction that is both legally significant and ethically indefensible. Türkiye operates three distinct digital regulatory instruments in parallel: Law No. 6698 on the Protection of Personal Data (PDPL), which establishes a GDPR-inspired rights-based data protection regime; Law No. 5651, which grants state authorities broad powers of content removal and platform blocking; and the draft amendment to Law No. 4054 on the Protection of Competition, which proposes a Digital Markets Act-inspired gatekeeper framework for digital markets. These three instruments have been enacted, amended, and developed in relative isolation from one another. No existing scholarship has subjected them to unified analysis. This article does so for the first time, applying Kantian deontological theory as the evaluative framework.

The choice of Kantian deontology is deliberate and methodologically justified. Kant's categorical imperative, specifically its second formulation, requiring that persons always be treated as ends in themselves and never merely as means, provides a precise and non-arbitrary standard against which regulatory instruments can be evaluated.³ Unlike consequentialist frameworks, which permit rights violations where aggregate welfare gains are sufficiently large, deontological analysis identifies whether a regulatory instrument structurally respects or violates the dignity and autonomy of the individuals it governs. This standard is particularly appropriate for digital regulation, where the central ethical question is not whether platforms produce net social benefits, but whether individuals retain meaningful control over their own data, expression, and digital agency.

The article proceeds as follows. Section I establishes the Kantian deontological framework and the specific evaluative criteria derived from it. Section II analyses

² Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through Such Publications (Türkiye), as amended by Law No. 7418 (18 October 2022), art 8A.

³ Immanuel Kant, *Groundwork of the Metaphysics of Morals* (Mary Gregor tr, Cambridge University Press 1997) 38 (4:429). The second formulation of the categorical imperative reads: "Act so that you treat humanity, whether in your own person or in that of another, always as an end and never as a means only."

PDPL through this framework, arguing that it partially but incompletely satisfies deontological requirements. Section III analyses Law No. 5651, arguing that its administrative blocking powers constitute a structural violation of deontology. Section IV analyses the draft amendment to Law No. 4054, arguing that its silence on individual rights constitutes a critical deontological omission. Section V synthesises the tripartite contradiction and argues that it is the precise reason Türkiye has not obtained EU adequacy recognition under Article 45 of the GDPR. Section VI concludes with concrete reform recommendations.

The contribution of this article is threefold. First, it provides the first unified ethical analysis of Türkiye's three principal digital regulatory instruments. Second, it demonstrates that the internal contradiction between these instruments is not subsidiary but structural, a product of legislative design choices that prioritised market regulation and state security over individual dignity. Third, it argues that resolving this contradiction is not merely an academic exercise but a precondition for Türkiye's meaningful integration into the European digital governance order.⁴

I. KANTIAN DEONTOLOGY AS THE EVALUATIVE FRAMEWORK

The choice of Kantian deontological theory as the evaluative framework for this analysis requires justification. Three reasons support this choice specifically in the context of digital regulation.

First, deontological ethics evaluates the structure of rules rather than their consequences. Digital regulation governs not individual acts but entire systems, data-processing architectures, content-moderation regimes, and platform-access rules, all of which affect millions of people simultaneously and whose harms are often diffuse, cumulative, and causally remote from any single decision. Consequentialist frameworks struggle to evaluate such systems because their aggregate effects are empirically uncertain and methodologically contested. Kantian deontology, by contrast, asks a prior question: does this regulatory instrument respect or violate the dignity and autonomy of the persons it governs, regardless of its outcomes? That question can be answered from the structure of the instrument itself.⁵

⁴ Türkiye has not received an EU adequacy decision under GDPR Article 45 as of the date of this article. The European Commission has not initiated a formal adequacy assessment for Türkiye. See European Commission, 'Adequacy Decisions' https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed 1 May 2026.

⁵ Onora O'Neill, *A Question of Trust: The BBC Reith Lectures 2002* (Cambridge University Press 2002) 115. O'Neill's argument that trust in institutions requires evaluating their structural commitments rather than their stated intentions underpins the methodological choice here. See also Roger Brownsword, *Law, Technology and Society: Reimagining the Regulatory Environment* (Routledge 2019) 45–47.

Second, Kantian deontology offers a stable standard for cross-jurisdictional analysis precisely because its central principle, the categorical imperative, is universal and admits no derogation. It does not permit derogation for reasons of cultural relativism, national security, or economic development. This universality allows the article to evaluate regulatory choices across jurisdictions, including Türkiye, without privileging any particular legal tradition.⁶

Third, Kantian deontology has gained prominence in digital governance scholarship, providing a methodological foundation for this article. Spahn has demonstrated that Kantian deontology, specifically its criteria of epistemic, motivational, and deliberative rationalism, generates concrete evaluative criteria for assessing digital behaviour change technologies, including regulatory instruments that shape how individuals form preferences and make decisions in digital environments.⁷

A. The Categorical Imperative and Its Two Operative Formulations

Kant articulated the categorical imperative in several formulations in the *Groundwork of the Metaphysics of Morals* (1785). Two are operative for this article's analysis.

The first formulation, the Formula of Universal Law, requires that one act only according to that maxim whereby one can, at the same time, will that it should become a universal law.⁸ Applied to regulation, this formulation asks: could the regulatory instrument under examination be universalised, that is, could every state coherently adopt the same instrument without generating a self-defeating contradiction? A censorship regime that depends for its legitimacy on the existence of free expression elsewhere, or that claims to protect privacy while simultaneously enabling state surveillance, fails this test because universalising it would destroy the very conditions that make it defensible.

The second formulation, the Formula of Humanity, requires that one act to treat humanity, whether in one's own person or in that of another, always as an

⁶ Christine M Korsgaard, 'Introduction' in Immanuel Kant, *Groundwork of the Metaphysics of Morals* (Mary Gregor tr, Cambridge University Press 1997) ix, xxiv. Korsgaard observes that the categorical imperative's universality is precisely what distinguishes it from culturally contingent moral standards.

⁷ Andreas Spahn, 'Digital Objects, Digital Subjects and Digital Societies: Deontology in the Age of Digitalisation' (2020) 11(4) *Information* art 228, DOI 10.3390/info11040228. Spahn identifies epistemic rationalism (the criterion that agents have access to accurate information about the choices they face), motivational rationalism (the criterion that agents' preferences are formed without manipulation), and deliberational rationalism (the criterion that agents can reflect on and revise their choices) as the three operative Kantian criteria for evaluating digital regulatory instruments.

⁸ Kant, *Groundwork* (n 3) 31 (4:421).

end and never merely as a means.⁹ This formulation is the primary evaluative instrument of this article. It generates a specific, operationalisable question about each of Türkiye's three digital regulatory instruments: does the instrument treat Turkish digital citizens as autonomous agents whose communicative choices, data, and digital identities are intrinsically valuable, or does it treat them as means to state security, market efficiency, or international regulatory optics?

B. Three Deontological Criteria Derived from the Categorical Imperative

To evaluate Türkiye's three regulatory instruments, this article derives three specific deontological criteria from the categorical imperative. This article does not invent these criteria; they are derived from Kant's own text and from the scholarly literature applying Kantian theory to digital governance.¹⁰

Criterion 1 - Autonomy preservation: A regulatory instrument reflects Kantian principles to the extent that it actively preserves and protects individuals' capacity to make informed, uncoerced choices about their own data, expression, and digital participation. Instruments that systematically undermine informed consent, restrict communicative freedom, or enable covert surveillance fail this criterion.

Criterion 2- Non-instrumentalisation: A regulatory instrument reflects Kantian principles to the extent that it does not treat individuals as instruments of state or market interests. Instruments that compel platforms to disclose user data to state authorities without individualised judicial authorisation, or that restrict user access to serve government communication strategies, fail this criterion.

Criterion 3- Universalisability: A regulatory instrument reflects Kantian principles to the extent that its underlying maxim can be universalised without contradiction. A state that claims to protect privacy in one statute while empowering administrative censorship in another cannot universalise its regulatory maxim; the contradiction is internal and deontologically disqualifying.

These three criteria will be applied consistently across Sections II, III, and IV to evaluate PDPL, Law No. 5651, and the draft amendment to Law No. 4054, respectively. The evaluations are not holistic assessments of Türkiye's regulatory intentions; they are structural analyses of whether each instrument's architecture, as enacted in its operative provisions, satisfies or violates the deontological standards derived above.

⁹ *ibid* 38 (4:429).

¹⁰ The derivation follows the methodological approach of Spahn (n 7). See also Luciano Floridi and others, 'An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28(4) *Minds and Machines* 689, 703–705.

C. What Deontological Analysis Does Not Claim

This article does not argue that Türkiye's government is acting in bad faith, that Turkish digital regulation is uniquely deficient, or that Kantian deontology is the only valid evaluative framework for digital governance. Regulatory systems in every jurisdiction contain internal tensions; the EU's own data protection framework has been criticised for privileging formal consent mechanisms over substantive autonomy.¹¹ The claim advanced here is narrower and more precise: that Türkiye's three digital regulatory instruments, analysed together through a Kantian deontological lens, reveal a structural contradiction that undermines their collective coherence and provides a principled explanation for Türkiye's failure to obtain EU adequacy recognition. That explanation has not previously been offered in the literature. Providing it is the contribution of this article.

II. PDPL: PARTIAL DEONTOLOGICAL ALIGNMENT

Türkiye's Law No. 6698 on the Protection of Personal Data, enacted on 7 April 2016 and amended most significantly in March 2024, represents the country's foundational commitment to rights-based digital governance.¹² Its stated purpose, to protect the fundamental rights and freedoms of persons, and in particular the privacy of personal life, while personal data is processed, is unambiguously deontological in orientation.¹³ Article 1 of the PDPL does not justify data protection on the grounds of economic efficiency, market confidence, or aggregate social welfare. It grounds protection in fundamental rights. That foundational choice reflects a Kantian intuition: that persons possess a dignity that cannot be traded against utility.

Measured against the three deontological criteria established in Section I, however, the PDPL's performance is partial rather than complete, and the gaps are structurally significant rather than merely technical.

On the first criterion, autonomy preservation, the PDPL makes a genuine and substantial contribution. Article 4 establishes six core processing principles that directly correspond to Kantian principles: lawfulness and fairness, purpose limitation, data minimisation, accuracy, storage limitation, and security and confidentiality.¹⁴ Article 3 defines explicit consent as freely given, specific, and informed, a formulation that mirrors the GDPR's consent standard and reflects the Kantian principle that autonomous choice must be uncoerced, particularised, and

¹¹ Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 *New York University Law Review* 771, 798–802.

¹² Law No 6698 on the Protection of Personal Data (Türkiye), Official Gazette No 29677, 7 April 2016 (PDPL), as amended by Law No 7499, Official Gazette No 32487, 2 March 2024.

¹³ PDPL (n 12) art 1.

¹⁴ *ibid* art 4.

based on adequate information.¹⁵ Article 11 grants data subjects a comprehensive set of rights, including the right to access their data, to request correction, to request deletion, and to object to processing. These rights treat the individual as an active agent in the governance of their own personal information rather than a passive object of administrative management.¹⁶

These provisions satisfy the autonomy preservation criterion in architectural terms. A legal system that defines consent as freely given and specific, that grounds data protection in fundamental rights rather than regulatory efficiency, and that vests enforceable rights in individual data subjects has taken the Kantian position seriously. It has, in principle, designed a framework that treats persons as ends in themselves.

However, the PDPL's satisfaction with the autonomy preservation criterion is undermined by a persistent and well-documented implementation gap. The PDPL Board, the independent supervisory authority established under Article 22, has issued inconsistent enforcement decisions, particularly regarding the public sector.¹⁷ Kantian deontology does not distinguish between private and public actors when applying the categorical imperative: a state institution that processes citizens' personal data without an adequate legal basis violates their autonomy no less than a private corporation does. A regulatory framework that applies its protections more rigorously and asymmetrically to private data controllers than to public authorities cannot claim full deontological compliance, regardless of its legislative text.

The 2024 amendments to Article 9, which introduced adequacy decisions, standard contractual clauses, and binding corporate rules for cross-border data transfers, represent a significant step toward closing the gap between the PDPL and GDPR standards.¹⁸ The amendments signal Türkiye's continued alignment with the EU. However, as of the date of this article, the European Commission has not initiated a formal adequacy assessment for Türkiye under GDPR Article 45, nor has any adequacy decision been issued.¹⁹ This absence is significant and

¹⁵ *ibid* art 3(a). The definition reads: "Explicit Consent: Freely given specific and informed consent."

¹⁶ *ibid* art 11.

¹⁷ Batu Kinikoglu, 'Implementing a New Data Protection Law: Lessons from the Turkish Experience' (2023) 13(1) *International Data Privacy Law* 25. Kinikoglu documents the PDPL Board's inconsistent enforcement record, particularly regarding public sector data controllers, and the absence of functional independence guarantees equivalent to GDPR Article 52

¹⁸ PDPL (n 12) art 9, as amended by Law No 7499 (n 12). The amended Article 9 introduced a three-tier transfer mechanism: adequacy decisions issued by the PDPL Board, appropriate safeguards including standard contractual clauses and binding corporate rules, and residual derogations for incidental transfers.

¹⁹ European Commission, 'Adequacy Decisions' (European Commission 2025) <https://>

will be examined in detail in Section V. For present purposes, it is sufficient to note that the 2024 amendments demonstrate legislative intent without yet producing the institutional consequence adequacy recognition that would confirm their effectiveness.

On the second criterion, non-instrumentalisation, the PDPL's record is more ambiguous. Article 28 of the PDPL exempts data processing carried out by public institutions for national security, defence, public safety, or the prevention of criminal offences from the law's general provisions.²⁰ The GDPR contains an analogous carve-out under Article 23, but the two exemption regimes differ in ways that extend well beyond the text of either provision.²¹ The GDPR's limitation regime is not a standalone proportionality clause. It is a jurisprudential architecture developed through three Grand Chamber judgments of the Court of Justice of the European Union. In *Digital Rights Ireland*, the Court established that data retention legislation must be strictly limited in scope, strictly necessary in application, and subject to independent oversight, invalidating the EU Data Retention Directive for exceeding the proportionality limits imposed by Articles 7, 8, and 52(1) of the Charter of Fundamental Rights.²² In *Tele2 Sverige*, the Court held that any national measure permitting state access to personal data must set out clear and precise rules, impose minimum safeguards against misuse, and provide for prior review by a court or an independent administrative authority, rather than merely ex post judicial control.²³ In *La Quadrature du Net*, the Court confirmed that general and indiscriminate retention of traffic and location data for national security purposes is precluded except where a Member State faces a real, present, or foreseeable serious threat, and only subject to temporal limitation and independent oversight.²⁴ PDPL Article 28 does not contain any of these constraints. It imposes no requirement of strict necessity, no minimum

commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed 1 May 2026.

²⁰ PDPL (n 12) art 28.

²¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data [2016] OJ L119/1 (GDPR), art 23(1). The GDPR requires that any legislative measure restricting data subject rights must 'respect the essence of the fundamental rights and freedoms' and must be 'a necessary and proportionate measure in a "democratic society."'

²² Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* EU:C:2014:238 (Grand Chamber, 8 April 2014) paras 39–71.

²³ Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* EU:C:2016:970 (Grand Chamber, 21 December 2016) paras 108–109.

²⁴ Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* EU: C:2020:791 (Grand Chamber, 6 October 2020) paras 135–140.

safeguards against misuse, and no obligation of prior independent review. The practical consequence is that Turkish public authorities may process citizens' personal data for broadly defined security purposes without the procedural architecture that three decades of CJEU jurisprudence has treated as the minimum condition of rights-compatible state access to personal data. Citizens whose data is processed under Article 28 are treated not as ends in themselves but as objects of state surveillance, the instrumentalisation that Kantian deontology prohibits.

The PDPL Board's capacity to remedy this deficit through enforcement is itself constrained by structural questions about its institutional independence. GDPR Article 52 requires that each supervisory authority act with complete independence, free from external influence. The PDPL Board's composition, with five of its nine members elected by the Grand National Assembly and two appointed by the Presidency, raises questions that any adequacy assessment would be required to examine.²⁵ It is important to note, however, that appointment by political bodies does not automatically compromise functional independence. France's CNIL, consistently regarded as one of the EU's most active and credible supervisory authorities, has 12 of its 18 members elected or designated by the Senate, the National Assembly, and the Supreme Courts.²⁶ The Bundestag appoints Germany's Federal Commissioner for Data Protection. What distinguishes these authorities from the PDPL Board is not their appointment model but the functional independence guarantees surrounding it: fixed terms, removal only for cause, explicit statutory prohibitions on seeking or receiving instructions, and institutional insulation from the executive branch. The PDPL Board lacks equivalent provisions for functional independence in its operative text. The independence deficit, where it exists, is therefore not a product of appointment method alone but of the absence of the institutional architecture that makes independence real rather than nominal.

On the third criterion, universalisability, the PDPL faces its most significant structural challenge. However, the nature of that challenge only becomes fully visible when the PDPL is read alongside Law No. 5651. The PDPL's regulatory maxim, that personal data shall be processed only with consent or on specified lawful grounds, and that individuals shall retain enforceable rights over their data, is universalisable in principle. No logical contradiction arises from imagining a

²⁵ PDPL (n 12) art 22(2). Five members of the Board are elected by the Grand National Assembly of Türkiye, two by the Presidency, and two by the Council of Ministers.

²⁶ Commission nationale de l'informatique et des libertés (CNIL), 'Status and Composition' <https://www.cnil.fr/en/cnil/status-composition> accessed 1 May 2026. The CNIL is an independent administrative authority composed of a college of 18 members, 12 of whom are elected or designated by the national authorities and courts to which they belong, including the Senate, the National Assembly, the Supreme Civil and Administrative Courts, and the Court of Auditors.

world in which every state adopted equivalent protections. The problem is that Türkiye has not adopted the PDPL on its own. It has simultaneously enacted Law No. 5651, whose operative provisions are structurally inconsistent with the PDPL's universalisable maxim. The universalisability analysis of the PDPL, therefore, cannot be completed in isolation; it requires the tripartite analysis provided by Sections III and IV.

The assessment of the PDPL under Kantian deontological theory produces a conclusion that is neither dismissive nor uncritical. The law is not deontologically deficient in the way that a cynically designed surveillance statute would be. Its foundational commitments to autonomy, consent, and individual rights reflect genuine engagement with the deontological tradition. Its structural weaknesses, the asymmetric application of its protections, the absence of the institutional architecture surrounding GDPR Article 23, and the implementation gap between legislative text and enforcement practice are real but remediable. What cannot be remedied within the PDPL itself is the external contradiction created by Law No. 5651, to which this article now turns.

III. LAW NO. 5651: STRUCTURAL DEONTOLOGICAL VIOLATION

The earthquake blocking introduced in Section I is not repeated here. It is invoked for a single purpose: as empirical proof that the deontological violation this section identifies in Law No. 5651 is not theoretical. Citizens denied access to the platform through which they sought rescue were not treated as autonomous agents whose communicative capacity constitutes a fundamental expression of dignity. They were treated as objects of an administrative decision made without their participation, without individualised justification, and without meaningful prior judicial oversight. That is the Kantian violation, not an incidental feature of Law No. 5651, but the direct consequence of its operative design.

Law No. 5651 is Türkiye's primary instrument for regulating internet content, enacted in 2007 and amended three times, progressively expanding the state's administrative power over digital platforms.²⁷ Its central provision for this analysis is Article 8A, which authorises the BTK to order the removal of content or the blocking of access to platforms in circumstances where delay would entail risk, on grounds including national security and public order, without prior judicial authorisation.²⁸ The Venice Commission examined Article 8A and found that appeal mechanisms are confined to review by a peace judgeship, that peace

²⁷ Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through Such Publications (Türkiye), enacted 4 May 2007, as amended by Law No. 6518 (2014), Law No. 7253 (29 July 2020), and Law No. 7418 (18 October 2022).

²⁸ *ibid* art 8A. Article 8A is titled 'Removal of content and/or blocking of access in circumstances where delay would entail risk'. It authorises the BTK to act on the initiative of specified ministries without prior judicial order, subject to *ex post* review.

judgeship decisions cannot be appealed to the Court of Cassation, and that many blocking decisions have been issued without adequate reasoning, rendering the ex post judicial control that the provision nominally provides largely ineffective in practice.²⁹ The practical consequence is an administrative power to silence platforms, exercisable with speed, breadth, and accountability so thin as to be structurally nominal.

Measured against the three deontological criteria established in Section II, Law No. 5651 fails each criterion in distinct and compounding ways.

On the first criterion, autonomy preservation, the failure is direct. The PDPL's consent standard, established in Section II, treats communicative and informational autonomy as a right to be actively protected. Article 8A operates on an entirely different logic: it authorises the state to remove the communicative infrastructure through which that autonomy is exercised, without the consent or participation of the individuals affected. A citizen whose access to a platform is blocked under Article 8A has not been individually notified, has not consented, and has no meaningful prior remedy. The autonomy that the PDPL promises in the domain of data processing is negated by a statute enacted by the same legislature and operating simultaneously in the same digital environment, in the domain of communicative freedom. Two instruments enacted by the same legislature, operating simultaneously in the same digital environment, rest on irreconcilable premises: one treats communicative autonomy as a right to be protected, the other as an infrastructure to be controlled.

The 2022 amendments compounded this violation by introducing Article 7A, which created a criminal offence for publicly disseminating false information about national security, public order, or public health in a way that could cause public unrest, carrying imprisonment of one to three years, extendable to five years for anonymous dissemination.³⁰ The Venice Commission and the Council of Europe Commissioner for Human Rights both found that Article 7A is incompatible with Article 10 of the European Convention on Human Rights.³¹ The provision was enacted three months before the 2023 Turkish general and

²⁹ Venice Commission (Council of Europe), *Opinion on Law No 5651* (CDL-AD(2016)011, 2016) paras 43–58 [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2016\)011-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)011-e) accessed 1 May 2026.

³⁰ Law No. 7418 (n 27), inserting art 217A into the Turkish Penal Code (TCK). Imprisonment of one to three years, extendable to three to five years, where the offence is committed anonymously or through media organisations.

³¹ Council of Europe Commissioner for Human Rights, *Letter to the Speaker of the Grand National Assembly of Türkiye* (CommHR/DM/sf 062-2022, 4 October 2022); Reporters Without Borders, *Turkey: RSF Condemns Adoption of Disinformation Law* (RSF, 13 October 2022) <https://rsf.org/en/Turkiye-rsf-condemns-adoption-disinformation-law> accessed 1 May 2026.

presidential elections. Its chilling effect on political expression is not speculative. Meta's transparency reports for 2024 document that Instagram complied with 79.15% of Turkish content removal requests, Facebook with 42%, and TikTok with 91.8%.³² These figures represent the systematic operation of a statutory architecture whose practical function is the suppression rather than the protection of communicative autonomy, the criterion that Kantian analysis requires digital regulation to honour.

On the second criterion, non-instrumentalisation, the violation lies in Law No. 5651's data localisation requirement, introduced by the 2020 amendments, which compels social network providers with over one million daily Turkish users to store Turkish user data on domestic servers.³³ The stated justification is regulatory oversight and consumer protection. The structural effect is categorically different: Turkish user data becomes more readily accessible to law enforcement and prosecutors, who may confiscate it from domestic servers without the procedural barriers that apply to data held abroad.³⁴ Citizens whose data is generated through the exercise of communicative autonomy find that same data made available to state actors as a byproduct of a regulatory architecture nominally designed for their protection. The gap between stated legislative purpose and structural operational effect is precisely what Kantian non-instrumentalisation analysis exists to identify. When a regulatory instrument treats citizens' data not as an expression of their dignity but as a resource for state surveillance, it fails the second formulation of the categorical imperative regardless of its formal justification.

On the third criterion, universalisability, the failure is comprehensive. The maxim underlying Article 8A that an administrative authority may silence digital platforms without prior judicial authorisation on broadly defined grounds of national security cannot be universalised without contradiction. Law No. 5651's own justificatory framework claims that restrictions on expression are permissible only where necessary and proportionate in a democratic society. That claim presupposes a democratic constitutional order characterised by judicial oversight, proportionality review, and meaningful appeal rights. Article 8A's operative structure systematically erodes each of those preconditions. A law that legitimates itself by reference to democratic standards while structurally

³² Human Rights Watch, *Joint Open Letter to Social Media Companies on Censorship in Turkey* (HRW, 8 May 2025) <https://www.hrw.org/news/2025/05/08/joint-open-letter-social-media-companies-censorship-turkiye> accessed 1 May 2026, citing Meta Transparency Report (January–December 2024) and TikTok Transparency Report (January–June 2024).

³³ Law No. 7253 (n 27), inserting Supplemental art 4 into Law No. 5651.

³⁴ Reset DOC, 'Turkey's New Internet Law and Its Effects on Freedom of Media' (Reset DOC, 2021) <https://www.resetdoc.org/story/Türkiye-internet-law-freedom-media/> accessed 1 May 2026.

undermining them cannot survive the universalisability test. Its maxim destroys the conditions of its own validity.

This analysis does not hold that all content regulation is impermissible under Kantian theory. Kant's political philosophy permits restriction of freedom where necessary to protect the equal freedom of others under a universal law.³⁵ The regulation of child sexual abuse material or direct incitement to violence satisfies this standard because those restrictions protect the dignity of identifiable victims and can be universalised without contradiction. What Article 8A and Article 7A authorise the administrative blocking of platforms on undefined public order grounds and the criminalisation of expression that causes undefined public unrest cannot be grounded in the protection of any individual's equal freedom and therefore cannot be reconciled with the categorical imperative.

Law No. 5651, in its current form, contains provisions whose architecture is structurally incompatible with the deontological commitments that the PDPL, enacted by the same legislature, formally endorses. That incompatibility is the product of deliberate legislative choices that prioritised state security and administrative convenience over individual dignity and communicative autonomy. Section V examines whether the draft Law No. 4054 amendment resolves this contradiction, compounds it, or, as this article argues, ignores it entirely.

IV. THE DRAFT LAW NO. 4054 AMENDMENT: DEONTOLOGICAL SILENCE AND THE COMPOUNDING OF CONTRADICTION

The draft amendment to Law No. 4054 on the Protection of Competition occupies a paradoxical position in Türkiye's digital regulatory landscape. It is simultaneously the most technically sophisticated of the three instruments under analysis and the most deontologically impoverished. The PDPL grounds its framework in fundamental rights. Law No. 5651 at least acknowledges freedom of communication, even as it systematically undermines it. The draft amendment to Law No. 4054 acknowledges neither. The amendment conceives of digital governance exclusively as a market structure problem. Its silence on individual rights is the product of that framing, deliberate, not incidental. That framing choice compounds the existing contradiction between PDPL and Law No. 5651 by adding a third instrument that validates the fiction of regulatory coherence.

The draft amendment, first published for public consultation in October 2022 and revised in November 2023 and June 2024, remains unenacted as of the date of this article, a fact that is itself analytically significant and is addressed below.³⁶ Its central mechanism is the designation of firms as undertakings holding

³⁵ Immanuel Kant, *The Metaphysics of Morals* (Mary Gregor tr, Cambridge University Press 1996) 24–26 (6:230–232).

³⁶ Cleary Gottlieb, *Digital Markets Regulation Handbook: Türkiye* (Cleary Gottlieb 2025)

significant market power in core platform services, a concept functionally equivalent to the European Union's DMA gatekeeper classification, based on quantitative thresholds including annual gross revenue and number of Turkish users, supplemented by qualitative criteria including network effects, data ownership, vertical integration, and conglomerate structure.³⁷ Designated firms would be subject to a list of ex ante obligations closely modelled on the DMA, including prohibitions on self-preferencing, restrictions on using non-public data when competing with business users, interoperability requirements, and obligations to provide users with continuous access to their personal data.³⁸ The structural parallels with the DMA are deliberate and extensively documented.³⁹

What is equally deliberate, and far less extensively examined, is what the draft amendment does not contain. The DMA operates within an EU legal order in which the Charter of Fundamental Rights is binding, the GDPR imposes non-derogable data protection obligations on designated gatekeepers, and the Court of Justice of the European Union exercises jurisdiction to ensure that competition remedies do not disproportionately restrict fundamental freedoms.⁴⁰ That relationship between competition law and data protection is not merely architectural, it is doctrinal. In *Meta Platforms v Bundeskartellamt*, the Court of Justice confirmed that a national competition authority may find a violation of the GDPR in the course of investigating an abuse of dominant position, establishing that data protection standards constitute normative constraints within competition law analysis.⁴¹ Costa-Cabral and Lynskey's foundational analysis demonstrates that when the material scope of data protection and competition law overlap, competition law can incorporate data protection as a normative yardstick for assessing non-price competition; data protection thus acts as an

<https://content.clearygottlieb.com/antitrust/digital-markets-regulation-handbook/turkey/index.html> accessed 1 May 2026.

³⁷ Turkish Competition Authority, *Draft Amendment to Law No 4054 on the Protection of Competition* (October 2022, revised November 2023 and June 2024), proposed art 8/A. See Kluwer Competition Law Blog, 'A New Age for Digital Markets in Turkey? The Draft Amendment to the Law No 4054 on the Protection of Competition' (25 October 2022)

³⁸ *ibid.* The draft amendment's obligations include prohibitions on using non-public data when competing with business users, self-preferencing restrictions, interoperability requirements, and obligations to give users continuous access to their personal data.

³⁹ Meredith Broadbent and John Strezewski, 'Turkey Considering New Digital Competition Legislation' (CSIS, May 2024) <https://www.csis.org/analysis/turkey-considering-new-digital-competition-legislation> accessed 1 May 2026.

⁴⁰ Charter of Fundamental Rights of the European Union [2000] OJ C364/1, arts 7–8; Regulation (EU) 2016/679 (GDPR) (n 21), arts 17–22.

⁴¹ Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* EU: C:2023:537 (Grand Chamber, 4 July 2023) paras 47–52.



internal constraint on what competition remedies may legitimately require.⁴² The draft amendment to Law No. 4054 fails to reflect any of this doctrinal development. It imposes DMA-equivalent obligations on digital platforms in a jurisdiction where, as Sections II and III have demonstrated, the data protection framework includes an unenforced public-sector exemption and the internet regulation framework authorises administrative censorship without prior judicial oversight. The draft amendment fails to ensure consistency between its gatekeeper obligations and PDPL data protection principles. It carves out no exemption for the BTK's administrative powers under Law No. 5651. The data portability and interoperability obligations it imposes provide no mechanism to ensure they serve individual privacy rather than expose it.

Measured against the three deontological criteria established in Section I, the draft amendment's performance is distinctive in kind rather than merely in degree from the failures identified in Section III.

On the first criterion, autonomy preservation, the draft amendment neither satisfies nor violates it directly. Its obligations, data portability, interoperability, and prohibition on self-preferencing are, in principle, autonomy-enhancing: users who can port their data between platforms and access competing services without artificial barriers have more meaningful choices than users locked into a single gatekeeper's ecosystem. That potential is real. However, it is unrealised in the draft amendment's current form because the instrument contains no mechanism for ensuring that autonomy gains at the competition layer translate into autonomy protections at the individual rights layer. A Turkish user whose data is made portable by a gatekeeper obligation under the draft amendment remains simultaneously subject to data localisation requirements under Law No. 5651 that make that same data accessible to state authorities. The autonomy gain and the autonomy loss operate in parallel, governed by instruments that have never been required to speak to each other. A deontologically coherent framework would evaluate competition obligations and surveillance powers together, as components of a single system answerable to the individual's communicative and informational agency.

On the second criterion, non-instrumentalisation, the draft amendment's silence is most consequential. The DMA's gatekeeper obligations exist, in the EU framework, within a broader normative architecture that treats individuals as the ultimate beneficiaries of competition policy, not merely as consumers whose welfare is measured by price and choice, but as rights-holders whose dignity sets limits on how their data may be used even within a competitive

⁴² Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection of Data Protection and Competition Law in EU Law' (2017) 54(1) *Common Market Law Review* 11, 11–14.

market.⁴³ The draft amendment to Law No. 4054 contains no equivalent normative foundation. Its preamble identifies the problem it addresses as the increasing power of gatekeepers in digital markets and the unfair practices this generates against business users, a framing that treats individuals primarily as consumers rather than as autonomous persons.⁴⁴ The remedy it proposes, *ex ante* behavioural obligations on designated firms, is designed to restore competitive market conditions, not to protect individual dignity. Competition law is not designed to be a rights instrument, and this article does not treat it as one. The criticism is of a legislature that adds a third digital regulatory instrument without asking whether it is consistent with the deontological commitments embedded, however imperfectly, in its first. The result is an instrument that treats Turkish digital citizens as market participants whose welfare is measured by competitive outcomes, in a jurisdiction where Law No. 5651 simultaneously treats them as subjects of administrative censorship whose communicative freedom is contingent on state tolerance. The Kantian principle that persons be treated as ends in themselves demands that a regulatory framework account for both dimensions simultaneously — a demand the draft amendment structurally refuses.

On the third criterion, universalizability, the draft amendment presents the most intellectually interesting failure of the three instruments under analysis. Its underlying maxim, which states that states may impose asymmetric *ex ante* obligations on dominant digital platforms to restore competitive market conditions, is, in principle, universalisable. The DMA demonstrates that multiple jurisdictions can adopt this maxim without logical contradiction; indeed, its universalisation is arguably desirable for the coherence of global digital markets. The universalisability failure of the draft amendment to Law No. 4054 is not in its competition law maxim considered in isolation. It is in the combined maxim that results from operating the draft amendment alongside Law No. 5651 simultaneously. The combined maxim produces an internal contradiction: a state imposes competition obligations to enhance user choice while simultaneously reserving unreviewable administrative power to block the same platforms without judicial oversight. That combined maxim cannot be universalised. A world in which every state both required platform interoperability for competitive reasons and reserved the right to block platform access for administrative reasons would be one in which competition obligations served no coherent purpose, because the access rights they created could be nullified at will by the same state that created them. The contradiction is not within the draft amendment. It is between the draft amendment and the instrument it refuses to acknowledge.

⁴³ Ariel Ezrachi and Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press, 2016) 211–215.

⁴⁴ Turkish Competition Authority (n 37), general preamble.

The fact that the draft amendment remains unenacted after more than two years of consultation is itself deontologically significant.⁴⁵ It reflects a legislative process that has prioritised formal alignment with the EU competition architecture, for the reputational and market-access benefits that alignment signals, without undertaking the harder work of ensuring that the proposed instrument is coherent with the rights framework that EU digital governance presupposes. Türkiye is, in effect, attempting to purchase the legitimacy of EU-style digital competition regulation without paying the price of EU-style individual rights protection. That purchase cannot be completed. As Section V demonstrates, it is precisely this attempt to claim EU alignment at the regulatory surface while maintaining structural deontological contradictions beneath it that explains Türkiye's continued failure to obtain EU adequacy recognition and defines the reform agenda this article proposes.

V. THE TRIPARTITE CONTRADICTION AND THE EU ADEQUACY FAILURE: SYNTHESIS AND REFORM RECOMMENDATIONS

The preceding three sections have demonstrated that Türkiye operates three digital regulatory instruments simultaneously: a data protection law that partially honours deontological principles, an internet regulation law that structurally violates them, and a draft competition amendment that is deontologically silent. Each instrument has been evaluated individually against the three criteria derived from Kantian deontology in Section I. This section performs a different analytical task. It asks what the three instruments reveal when read together as a system rather than as a collection of separate statutes. It argues that the answer to that question provides the first principled explanation for a fact noted but inadequately theorised in the existing literature: Türkiye's continued failure to obtain EU adequacy recognition under GDPR Article 45.

The EU adequacy framework is not a diplomatic instrument. It is a legal assessment governed by Article 45 of the GDPR, which requires the European Commission to evaluate whether a third country ensures an adequate level of protection for personal data transferred from the EU. The standard is not identical to legislation. The Commission has confirmed that the principle of essential equivalence, as clarified by the Court of Justice of the European Union in its Schrems II judgment, requires that the third country's overall data protection system achieve protection that is in substance equivalent to that guaranteed in the EU legal order.⁴⁶ Article 45(2) specifies the criteria the Commission must

⁴⁵ Information Technology and Innovation Foundation (ITIF), 'Comments Before the Turkish Competition Authority Regarding Act No 4054 on the Protection of Competition' (ITIF, 10 June 2024) <https://itif.org/publications/2024/06/10/comments-before-the-turkish-competition-authority-regarding-act-4054/> accessed 1 May 2026.

⁴⁶ Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilian*

assess: the rule of law; respect for human rights and fundamental freedoms; relevant legislation, including concerning national security and the access of public authorities to personal data; the existence and effective functioning of an independent supervisory authority; and the existence of effective and enforceable data subject rights with effective judicial redress.⁴⁷

Türkiye satisfies none of these criteria fully, and this article's tripartite analysis explains precisely why. The PDPL's provisions are formally comparable to GDPR standards in several important respects. The failure, however, is structural: it is the product of an internal regulatory contradiction that prevents any of the three instruments from functioning as their texts suggest, since the others undermine each other.

Before proceeding to that structural analysis, one dimension of Türkiye's adequacy position requires acknowledgement. The adequacy decision process involves both legal assessment and political judgment. Türkiye's PDPL Board has conditioned its own adequacy decisions on reciprocity, meaning Türkiye will declare a country adequate only if that country has first declared Türkiye adequate.⁴⁸ The Turkish Ministry of Foreign Affairs has stated that, in any event and under all circumstances, any safe country decision should be based on reciprocity. This creates a political deadlock: the European Commission cannot issue an adequacy decision for Türkiye until Türkiye's legal framework meets the essential equivalence requirement, but Türkiye's PDPL Board will not issue adequacy decisions for EU Member States until the Commission acts first. This reciprocity dynamic is a political obstacle to the recognition of adequacy. The tripartite contradiction this article identifies, however, is a structural legal obstacle that would persist even if the political deadlock were resolved. A Commission adequacy assessment conducted in the absence of any reciprocity constraint would still confront the legal deficiencies identified in this section.

The rule-of-law requirement is the most fundamental. A legal system committed to the rule of law must ensure that restrictions on fundamental rights are prescribed by law, pursue a legitimate aim, and are necessary and proportionate

Schrems (Schrems II) EU: C:2020:559 (Grand Chamber, 16 July 2020) paras 94–97. The CJEU held that the standard of essential equivalence requires that the third country's legal system ensure a level of protection of fundamental rights and freedoms substantially equivalent to that guaranteed within the EU by the GDPR read in light of the Charter of Fundamental Rights.

⁴⁷ Regulation (EU) 2016/679 (GDPR) (n 21), art 45(2)(a)–(b).

⁴⁸ Batu Kinikoglu, 'Implementing a New Data Protection Law: Lessons from the Turkish Experience' (2023) 13(1) *International Data Privacy Law* 25, 39–40. Kinikoglu documents that the Turkish Ministry of Foreign Affairs stated that 'in any event and under all circumstances' any safe country decision should be based on reciprocity, and that the PDPL Board has relied on this principle to justify the non-publication of Türkiye's adequacy list for EU Member States.

in a democratic society. These are the standards set out in Article 10(2) of the European Convention on Human Rights, which the CJEU has treated as the minimum threshold for adequacy assessments involving restrictions on freedom of expression and privacy.⁴⁹ Law No. 5651's Article 8A fails this threshold on all three elements: blocking orders are issued on broadly defined grounds that give the BTK virtually unlimited discretion; the Venice Commission has found that the proportionality standard is absent from the operative provisions; and the appeal mechanism is so constrained, confined to a peace judgeship with no further recourse, that it does not constitute effective judicial redress. A Commission adequacy assessment examining Law No. 5651 alongside the PDPL would be compelled to conclude that Türkiye's overall legal system does not ensure that restrictions on communicative freedom meet rule-of-law standards, regardless of what the PDPL says about data protection.

The requirement for human rights and fundamental freedoms compounds this failure. The CJEU in *Schrems II* held that the essential equivalence standard requires the third country's legal system to guarantee, in practice and not merely in legislative text, that public authorities' access to personal data is limited to what is strictly necessary and subject to effective judicial oversight.⁵⁰ Türkiye's Article 28 PDPL exemption, which permits public authorities to process personal data for national security purposes without the proportionality constraints that the GDPR imposes on equivalent derogations, already falls short of this standard when examined in isolation. Law No. 5651's data localisation requirement transforms a partial shortfall into a systemic failure: not only may public authorities process citizens' data without proportionality review, but the regulatory architecture actively ensures that citizens' data is stored domestically in a form that maximises state accessibility. These two instruments are architecturally complementary rather than independently deficient, designed to operate together in ways that produce a surveillance infrastructure structurally incompatible with the essential equivalence standard.

The requirement for an independent supervisory authority presents a further obstacle. GDPR Article 45(2)(b) requires that the third country's supervisory authority possess genuine independence, adequate resources, and effective enforcement powers. The PDPL Board's composition, with five of its nine members elected by the Grand National Assembly and two appointed by the Presidency, raises structural questions about independence that the Commission would be

⁴⁹ European Convention on Human Rights, art 10(2). See also Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* (*Schrems I*) EU: C:2015:650 (Grand Chamber, 6 October 2015) para 95.

⁵⁰ *Schrems II* (n 46) paras 175–185.

required to examine.⁵¹ More fundamentally, an adequacy assessment would need to explain how a supervisory authority can effectively enforce data protection standards when a parallel statute, Law No. 5651, confers on the BTK powers to compel platform compliance and access to user data that operate entirely outside the PDPL Board's jurisdiction. Effective data protection supervision cannot coexist with an internet regulation framework whose enforcement architecture is structurally immune to data protection oversight.

The deontological analysis in this article aligns precisely with the adequacy criteria the Commission would apply. The Kantian criterion of preserving autonomy corresponds to the GDPR requirement for effective and enforceable data subject rights. The criterion of non-instrumentalisation corresponds to the requirement that public authority access to personal data be limited to what is strictly necessary. The criterion of universalisability corresponds to the requirement that restrictions on fundamental rights be prescribed by law and proportionate. Türkiye fails all three Kantian criteria in ways that map onto failures of all three adequacy standards. This mapping is not coincidental. It reflects that both Kantian deontology and the EU adequacy framework are grounded in the same foundational commitment to treating individuals as rights-holders whose dignity sets non-negotiable limits on what states and markets may do with their data and communicative freedom.

The draft amendment to Law No. 4054's deontological silence compounds this failure in a specific and practically significant way. Türkiye has invested substantial legislative and institutional resources in developing a DMA-equivalent competition framework for digital markets. Adequacy assessments, however, are not conducted based on signals. They examine the overall legal system. The DMA itself makes the relevant relationship explicit: Recital 7 establishes that the act complements the application of EU rules on the protection of personal data and privacy, including the GDPR, situating competition obligations within a fundamental rights architecture that treats data protection and market regulation as inseparable rather than parallel concerns.⁵² Türkiye's draft amendment to Law No. 4054 contains no equivalent provision. A competition framework that imposes DMA-equivalent obligations on digital platforms while operating alongside a censorship framework incompatible with ECHR Article 10 and remaining silent on its relationship to the PDPL does not create overall essential equivalence. It

⁵¹ PDPL (n 12) art 22(2). Five members of the Board are elected by the Grand National Assembly of Türkiye, two by the Presidency, and two by the Council of Ministers.

⁵² Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector [2022] OJ L265/1 (Digital Markets Act), Recital 7. Recital 7 states that the DMA complements, and does not prejudice, the application of Union rules on the protection of personal data and privacy, including the General Data Protection Regulation, the Directive on privacy and electronic communications.

creates a regulatory surface that mimics EU architecture while concealing the deontological contradictions that the adequacy assessment process is specifically designed to detect.

VI. REFORM RECOMMENDATIONS

This article's analysis generates three concrete legislative recommendations, each targeted at a specific instrument and derived directly from the deontological criteria identified in Section I. They are framed not as criticism of Turkish digital governance but as the minimum changes required to resolve the tripartite contradiction and establish the conditions for a credible EU adequacy assessment.

The first recommendation addresses Law No. 5651. Article 8A must be amended to require prior judicial authorisation for all platform blocking orders except in the most narrowly defined emergency circumstances, and to impose an explicit proportionality standard, equivalent to that in GDPR Article 23(1), on any restriction of communicative freedom that also constitutes a restriction of data subjects' ability to exercise their PDPL rights. Article 7A must be repealed or fundamentally revised to confine its scope to content that directly and imminently threatens the physical safety of identifiable individuals, the only restriction that Kantian principles and ECHR Article 10(2) jointly permit. These amendments would not prevent Türkiye from regulating harmful digital content. They would require that regulation to meet the proportionality standards that the rule of law and essential equivalence demand.

The second recommendation addresses the PDPL. Article 28's national security exemption must be amended to incorporate an explicit proportionality standard and to extend the PDPL Board's supervisory jurisdiction to cover public authority data processing, including processing carried out under Law No. 5651, without exception. This amendment would not prevent Turkish public authorities from accessing data for legitimate security purposes. It would require that access to be proportionate, individually authorised, and subject to genuine independent oversight, the conditions that the Schrems II essential equivalence standard demands and that the current framework structurally prevents.

The third recommendation addresses the amendment to draft Law No. 4054. Before enactment, the draft must be supplemented by an explicit coherence provision, modelled on Recital 7 of the DMA⁵³, requiring that gatekeeper obligations be interpreted and applied consistently with PDPL data protection principles and with the amended provisions of Law No. 5651. This provision would not alter the draft amendment's competition law substance. It would ensure that the three instruments operate as a coherent regulatory framework rather than as three independent statutes that share a jurisdiction but not a philosophy.

⁵³ DMA(n52) Recital 7

These three recommendations would not transform Türkiye into an EU member state or require it to adopt identical data protection standards. The essential equivalence standard does not demand identity. It demands coherence, a legal system in which the protection of individual dignity and communicative autonomy is not promised by one statute and systematically undermined by another. That coherence is achievable. It requires legislative will rather than legislative genius. Its achievement would serve Türkiye's own stated interest in European digital governance integration far more effectively than any amount of regulatory surface alignment without the deontological foundation to sustain it.

CONCLUSION

This article set out to do one thing that existing scholarship had not done: to analyse Türkiye's three principal digital regulatory instruments, the PDPL, Law No. 5651, and the draft amendment to Law No. 4054, together as a system, through a single evaluative framework derived from Kantian deontological theory. The analysis has produced four conclusions that, though logically independent of one another, converge on a single finding.

The first conclusion is that the PDPL, despite its genuine deontological ambitions, is structurally incomplete. Its foundational commitment to autonomy, consent, and individual rights reflects an authentic engagement with the Kantian tradition. Its Article 28 exemption, its asymmetric enforcement record, and the absence of a proportionality standard equivalent to GDPR Article 23(1) prevent it from meeting the deontological criteria this article has applied in full. The PDPL's deficiencies are remediable. They reflect incomplete institutional development rather than a framework designed to circumvent the rights it nominally protects.

The second conclusion is that Law No. 5651 is not unfinished. It is architecturally incompatible with deontological governance. Article 8A's administrative blocking power, Article 7A's criminalisation of broadly defined false information, and the data localisation requirement collectively fail all three deontological criteria. Citizens are denied communicative autonomy at the moments they most need it. Their data is instrumentalised for state surveillance. The maxim underlying these provisions destroys the democratic conditions that Law No. 5651's own justificatory framework presupposes. The earthquake blocking of February 2023 is the most viscerally legible demonstration of that failure. It is the system operating as designed.

The third conclusion is that the draft amendment to Law No. 4054's deontological silence is not a minor omission but a compounding failure. By adding a third instrument that models EU competition architecture while ignoring the rights framework that architecture presupposes, Türkiye has created a regulatory surface that signals alignment without delivering it. The combined maxim that results from operating all three instruments simultaneously cannot be universalised

without contradiction. The EU adequacy assessment process would be required to evaluate that combined maxim, not any single instrument in isolation.

The fourth and most significant conclusion is that Türkiye's failure to obtain EU adequacy recognition is not a diplomatic contingency or a negotiating gap. It is a structural deontological consequence. GDPR Article 45 requires the European Commission to assess four criteria: rule of law, respect for human rights, independent supervision, and effective judicial redress. Each maps precisely onto a Kantian criterion that this article has applied: autonomy preservation, non-instrumentalisation, and universalisability, respectively. Türkiye fails both sets of criteria for the same reason: its regulatory framework promises to protect individual dignity in one statute while systematically undermining the conditions of that protection in another. Essential equivalence cannot be achieved through legislative mimicry. Deontological coherence is the precondition: a legal system in which all three instruments operate as components of a single framework that treats Turkish digital citizens as ends in themselves rather than as objects of administrative management, market regulation, or state surveillance.

The three reform recommendations advanced in Section V, amending Article 8A and repealing Article 7A of Law No. 5651, extending PDPL Board jurisdiction to cover public authority processing without exception, and supplementing the draft Law No. 4054 amendment with an explicit coherence provision, are not proposals for Türkiye to become something it is not. They are the minimum changes required for Türkiye to become what its own legislation already claims it is: a jurisdiction committed to the fundamental rights and freedoms of its digital citizens. That commitment, once made structurally rather than merely textually, is the only foundation on which EU adequacy recognition, and the credibility of Türkiye's digital governance ambitions, can genuinely rest.

BIBLIOGRAPHY

Primary Legislation

Charter of Fundamental Rights of the European Union [2000] OJ C364/1

European Convention on Human Rights (as amended by Protocol No 14, CETS No 194, 2010)

Law No 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through Such Publications (Türkiye), enacted 4 May 2007, as amended by Law No 6518 (2014), Law No 7253 (Official Gazette No 31202, 29 July 2020), and Law No 7418 (Official Gazette No 31987, 18 October 2022)

Law No 6698 on the Protection of Personal Data (Türkiye) (PDPL), Official Gazette No 29677, 7 April 2016, as amended by Law No 7499, Official Gazette No 32487, 2 March 2024

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data [2016] OJ L119/1 (GDPR)

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector [2022] OJ L265/1 (Digital Markets Act)

Turkish Competition Authority, *Draft Amendment to Law No 4054 on the Protection of Competition* (October 2022, revised November 2023 and June 2024) (unenacted as of May 2026)

Turkish Penal Code (TCK), art 217A, inserted by Law No 7418 (Official Gazette No 31987, 18 October 2022)

Cases

Case C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* EU:C:2014:238 (Grand Chamber, 8 April 2014)

Case C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* EU:C:2016:970 (Grand Chamber, 21 December 2016)

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU: C:2015:650 (Schrems I)

Case C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* EU: C:2020:791 (Grand Chamber, 6 October 2020)

Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* EU: C:2023:537 (Grand Chamber, 4 July 2023)

Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* EU: C:2020:559 (Schrems II)

Books

Brownsword R, *Law, Technology and Society: Reimagining the Regulatory Environment* (Routledge 2019)

Ezrachi A and Stucke ME, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press, 2016)

Kant I, *Groundwork of the Metaphysics of Morals* (Gregor M tr, Cambridge University Press 1997)

Kant I, *The Metaphysics of Morals* (Gregor M tr, Cambridge University Press 1996)

Korsgaard CM, 'Introduction' in Kant I, *Groundwork of the Metaphysics of Morals* (Gregor M tr, Cambridge University Press 1997)

O'Neill O, *A Question of Trust: The BBC Reith Lectures 2002* (Cambridge University Press 2002)

Journal Articles and Other Sources

Akdeniz Y and Altıparmak K, *Turkey: Freedom of Expression in Jeopardy* (English PEN/PEN International 2020) https://www.englishpen.org/wp-content/uploads/2020/07/Turkey_Freedom_of_Expression_in_Jeopardy_ENG.pdf accessed 1 May 2026

Balamir Coskun G, 'Turkey's New Internet Law and Its Effects on Freedom of Media' (Reset DOC, 12 July 2021) <https://www.resetdoc.org/story/turkey-internet-law-freedom-media/> accessed 1 May 2026

Broadbent M and Strezewski J, 'Turkey Considering New Digital Competition Legislation' (CSIS, May 2024) <https://www.csis.org/analysis/turkey-considering-new-digital-competition-legislation> accessed 1 May 2026

Cleary Gottlieb, *Digital Markets Regulation Handbook: Türkiye* (Cleary Gottlieb 2025) <https://content.clearygottlieb.com/antitrust/digital-markets-regulation-handbook/turkey/index.html> accessed 1 May 2026

Commission nationale de l'informatique et des libertés (CNIL), 'Status and Composition' <https://www.cnil.fr/en/cnil/status-composition> accessed 1 May 2026

Costa-Cabral F and Lynskey O, 'Family Ties: The Intersection of Data Protection and Competition Law in EU Law' (2017) 54(1) *Common Market Law Review* 11

Council of Europe Commissioner for Human Rights, *Letter to the Speaker of the Grand National Assembly of Türkiye* (CommHR/DM/sf 062-2022, 4 October 2022)

European Commission, 'Adequacy Decisions' (European Commission 2025) https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed 1 May 2026

Floridi L and others, 'AI4People- An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28(4) *Minds and Machines* 689 <https://doi.org/10.1007/s11023-018-9482-5>

Freedom House, *Freedom on the Net 2024: Turkey Country Report* (Freedom House 2024) <https://freedomhouse.org/country/turkey/freedom-net/2024> accessed 1 May 2026

Human Rights Watch, *Joint Open Letter to Social Media Companies on Censorship in Türkiye* (HRW, 8 May 2025) <https://www.hrw.org/news/2025/05/08/joint-open-letter-social-media-companies-censorship-turkiye> accessed 1 May 2026

Information Technology and Innovation Foundation (ITIF), 'Comments Before the Turkish Competition Authority Regarding Act No 4054 on the Protection of Competition' (ITIF, 10 June 2024) <https://itif.org/publications/2024/06/10/comments-before-the-turkish-competition-authority-regarding-act-4054/> accessed 1 May 2026

Kinikoglu B, 'Implementing a New Data Protection Law: Lessons from the Turkish Experience' (2023) 13(1) *International Data Privacy Law* 25

Kişisel Verileri Koruma Kurumu (KVKK Board), 'Personal Data Protection Law' <https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law> accessed 1 May 2026

Kluwer Competition Law Blog, 'A New Age for Digital Markets in Turkey? The Draft Amendment to the Law No 4054 on the Protection of Competition' (25 October 2022) <https://competitionlawblog.kluwercompetitionlaw.com/2022/10/25/a-new-age-for-digital-markets-in-turkey-the-draft-amendment-to-the-law-no-4054-on-the-protection-of-competition/> accessed 1 May 2026

Reporters Without Borders, 'Turkey: International Delegation Condemns Passage of Disinformation Law' (RSF, 14 October 2022) <https://rsf.org/en/turkey-international-delegation-condemns-passage-disinformation-law-and-issues-call-protect-safety> accessed 1 May 2026

Schwartz PM, 'Global Data Privacy: The EU Way' (2019) 94 *New York University Law Review* 771

Spahn A, 'Digital Objects, Digital Subjects and Digital Societies: Deontology in the Age of Digitalisation' (2020) 11(4) *Information* art 228 <https://doi.org/10.3390/info11040228>

Venice Commission (Council of Europe), *Opinion on Law No 5651* (CDL-AD(2016)011, 2016) [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2016\)011-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)011-e) accessed 1 May 2026

