World Trade Review (2026), **25**, 556–582
doi:10.1017/S1474745626101578

ORIGINAL ARTICLE

Regulating Source Code in Trade Agreements: Between Protection and Disclosure

María Vásquez Callo-Müller

Faculty of Law, University of Lucerne, Switzerland
Email: maria.vasquez@unilu.ch

(Received 2 May 2025 UTC; revised 30 May 2026 UTC; accepted 15 June 2026 UTC)

Abstract

Provisions prohibiting the mandatory disclosure of source code and algorithms as a condition for market access in digital trade rulemaking aim to prevent forced technology transfer and safeguard confidential business information. However, their proliferation raises significant concerns regarding the state's capacity to regulate digital technologies, including artificial intelligence. This Article argues that their rapid diffusion signals a regime shift in the international protection of software and algorithms, from intellectual property (IP) law to digital trade law. Under the TRIPS framework, trade secrets primarily protect undisclosed confidential information, such as source code and algorithms, and offer limited protection at the point of market entry. Source code provisions in digital trade function as an ex-ante layer of protection that operates independently of, yet cumulatively with, existing IP rights. Because digital trade law lacks the internal balancing mechanisms characteristic of the IP regime, regulatory space is mediated principally through the design of exceptions and carve-outs. By situating these provisions against this background, this Article reframes current debates from regulatory chill to the governance consequences of this regime shift and contends that the design of source code exceptions and carve-outs is now the primary mechanism for balancing proprietary protection against legitimate public policy disclosure.

Keywords: Algorithms; artificial intelligence; digital trade; intellectual property; source code; TRIPS; trade secrets; trade agreements

1. Introduction

Non-disclosure of source code provisions in trade agreements are increasingly used to prohibit measures that require transfer of, and/or access to, software, source code, and, if applicable, algorithms, as a condition for market access. Initially promoted by major software-exporting economies,[1] and first appearing in the Japan–Mongolia Free Trade Agreement (FTA),[2] such a provision has been included in two South–South agreements, namely the Chile–Paraguay FTA of 2021,[3] and, more recently, in the

[1]See 'US Chamber of Commerce, Multi-Organization Letter Urges USTR to Restore US Leadership on Digital Trade Rules', 3 March 2025, www.uschamber.com/international/trade-agreements/multi-organization-letter-urges-ustr-to-restore-us-leadership-on-digital-trade-rules (accessed 11 April 2025) (outlining the need to promote provisions on the non-disclosure of source code and algorithms in digital trade).

[2]Although, a WikiLeaks document shows that it was initially part of the Trade in Services (TiSA) Annex on Electronic Commerce, as proposed by Japan, see 'TiSA Annex on Electronic Commerce', Article 6, https://wikileaks.org/tisa/ecommerce/ (accessed 11 April 2025).

[3]Chile–Paraguay FTA, Article 7.16.

© The Author(s), 2026. Published by Cambridge University Press on behalf of The Secretariat of the World Trade Organization. This is an Open Access article, distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives licence (http://creativecommons.org/licenses/by-nc-nd/4.0), which permits non-commercial re-use, distribution, and reproduction in any medium, provided that no alterations are made and the original article is properly cited. The written permission of Cambridge University Press or the rights holder(s) must be obtained prior to any commercial use and/or adaptation of the article.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

African Continental Free Trade Agreement (AfCFTA) Digital Trade Protocol of 2024.[4] Other large regional economic integration projects involving developing countries and least developed countries (LDCs), such as the ASEAN Digital Economy Framework Agreement (DEFA), also considered the incorporation of a source code provision.[5] This diffusion indicates that source code provisions are no longer a niche demand of a small group of technologically advanced countries but an increasingly standard component of digital trade rulemaking.[6]

At the same time, these provisions remain controversial. The WTO Agreement on Electronic Commerce with Interim Arrangements,[7] the main output of the WTO Joint Statement Initiative on Electronic Commerce, does not feature a source code provision. This is partly due to the regulatory chill that such a provision allegedly poses on the ability of governments to regulate new technologies, including Artificial Intelligence (AI).[8] Academic studies have also highlighted potential risks, noting that these provisions may constrain the capacity of regulatory authorities to monitor software products originating from foreign jurisdictions,[9] thereby limiting the transparency, accountability, and effective regulatory oversight of software and increasingly algorithmic systems.[10] Source code provisions could, for instance, conflict with domestic legislation, such as the European Union (EU) AI Act,[11] and other proposed legislation in countries such as Argentina,[12] which include requirements to disclose software's source code during regulatory audits and conformity assessments. While these

[4]See 'African Continental Free Trade Agreement (AfCFTA) Digital Trade Protocol' (adopted in February 2024), and 'Dedicated Annex on Criteria for Determining the Legitimate and Legal Public Interest Reasons for Disclosure of Source Code' (AfCFTA Source Code Annex) (adopted February 2025), Article 24.

[5]As discussed in the capacity-building event for the ASEAN Digital Economy Framework Agreement (DEFA) negotiators, 4 February 2025, Kuala Lumpur, Malaysia.

[6]Indeed, these provisions form part of the cluster of issues in digital trade negotiations referred to as 'trust in digital transactions', particularly 'business trust'. See T. Nemoto and J. Lopez-Gonzalez (2021) 'Digital Trade Inventory: Rules, Standards and Principles', OECD Trade Policy Paper 251, 7.

[7]WTO Ministerial Conference Fourteenth Session, 'Declaration on Interim Arrangements for the Agreement on Electronic Commerce', WT/MIN(26)/42, 28 March 2026.

[8]Paradoxically, these concerns have been raised by the previous United States (US) administration. See Fireside chat with USTR Katherine Tai, Aspen Security Forum, 7 December 2023, www.aspensecurityforum.org/dc-2023-videos (accessed 11 April 2025) (noting that certain provisions in digital trade agreements, including on source code, amount to a 'policy suicide').

[9]AI Now Institute, 'International "Digital Trade" Agreements: The Next Frontier', 11 April 2023, https://ainowinstitute.org/publication/international-digital-trade-agreements/ (accessed 11 April 2025).

[10]See generally M. Słok-Wódkowska and J. Mazur (2022) 'Secrecy by Default: How Regional Trade Agreements Reshape Protection of Source Code', *Journal of International Economic Law* 25, 91; K. Irion (2022) 'Algorithms Off-Limits?: If Digital Trade Law Restricts Access to Source Code of Software then Accountability Will Suffer', 2022 ACM Conference on Fairness, Accountability, and Transparency, 1561; E. Jones et al. (2024) 'AI Governance and the Future of Digital Trade Policy: Options for the UK', Blavatnik School of Government Policy Brief, www.bsg.ox.ac.uk/sites/default/files/2024-10/Policy%20brief%20c%20AI%20governance%20and%20the%20future%20of%20digital%20trade%20policy.pdf (accessed 22 April 2025).

[11]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No. 300/2008 (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) OJ L, 2024/1689, 12 July 2024 EU AI Act). See also: Article 74 (13) (a) EU AI Act (on 'Market surveillance and control of AI systems in the Union market', providing that 'Market surveillance authorities shall be granted access to the source code of the high-risk AI system upon a reasoned request and only when both of the following conditions are fulfilled: (a) access to source code is necessary to assess the conformity of a high-risk AI system with the requirements set out in Chapter III, Section 2; and (b) testing or auditing procedures and verifications based on the data and documentation provided by the provider have been exhausted or proved insufficient'), and Article 98 EU AI Act (on the 'Power to conduct evaluations', providing that '1. The AI Office, after consulting the Board, may conduct evaluations of the general-purpose AI model concerned … 3. For the purposes of paragraph 1, the Commission may request access to the general-purpose AI model concerned through APIs or further appropriate technical means and tools, including source code')

[12]See Argentina, Proposed Legal Framework for the Regulation of the Development and Use of Artificial Intelligence, Article 16 (on the 'Registration of AI Systems', providing that 'Developers and providers of artificial intelligence systems shall fully cooperate with ASIA and provide access to their systems, source codes, data, and relevant documentation for the purposes of supervision and control.')

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

concerns are well-founded, due in part to the indeterminacy of key terms, such as 'source code' and 'algorithms', they have tended to overshadow a related but analytically distinct question: the linkage between the emergence of source code provisions in digital trade law and the deficiencies of the existing international intellectual property (IP) framework.

It is against this background that this article advances a different claim. It argues that source code provisions are best understood as part of a structural relocation (or 'shift') in the protection of software and algorithms from international intellectual property (IP) law to digital trade law. The Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement[13] achieves the protection of source code and algorithms only indirectly (primarily through the protection offered by TRIPS Article 39 concerning 'undisclosed information' or 'trade secrets'). Yet, this protection remains insufficient as TRIPS Article 39.2 applies to misappropriation in the context of unfair competition (the functional scope of trade secret protection under TRIPS) and furthermore does not protect information submitted to the government. TRIPS-plus agreements similarly do not offer sufficient protection. Source code provisions in digital trade rulemaking emerged as a result of these deficiencies and are a functional response to the inability of the international IP regime to evolve in tandem with technological and commercial realities of cross-border trade in software and AI systems, where concerns about compelled government-mandated disclosure arise at the stage of market entry,[14] beyond those associated with commercial misappropriation. They establish an ex-ante obligation not to require the transfer of, or access to, source code as a condition for importation, distribution, sale, or use of software and software-embedded products, namely a ban on mandatory source code disclosure. This obligation applies irrespective of whether the relevant source code or, if applicable, the algorithm qualifies for protection under IP law. Where source code, and if applicable, algorithms, are already protected as trade secrets (or other IP rights), these provisions may operate cumulatively, adding an extra layer of protection.

The above has systemic implications. Unlike IP law, digital trade disciplines on source code do not operate within a general framework of balance of rights and obligations,[15] where proprietary interests are, by design, balanced against public regulatory objectives. As a result, the internal flexibilities of the IP regime, for instance, the definition of the protected subject matter, can no longer secure regulatory space for source code and algorithm regulation.[16] Instead, the design and interpretation of exceptions and carve-outs in digital trade law becomes the central mechanism through which the balance between protection and disclosure will be determined.

This Article examines this issue through a systematic analysis of all existing source code provisions in digital trade chapters in FTAs and Digital Economy Agreements (DEAs) to date. Trade secret rules in FTA IP chapters are also studied using the Trade Agreements Provisions on Electronic Commerce and Data (TAPED) dataset.[17] On that basis, it analyses the interface between the two regimes that have thus far evolved separately, assessing the policy implications of this ongoing domain shift. In doing so, it highlights the need to better understand the mechanisms to protect regulatory autonomy

[13] Agreement on Trade-Related Aspects of Intellectual Property Rights, 15 April 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 UNTS. 299, 33 ILM 1197 (1994). (TRIPS)

[14] See generally, A. Andrenelli et al. (2019) 'International Technology Transfer Policies', OECD Trade Policy Papers vol. 222, 8.

[15] TRIPS, Article 7 (Objectives).

[16] A. Taubman et al. (eds) (2012) *A Handbook on the WTO TRIPS Agreement*. Cambridge University Press, 4 (noting that '[IPRs] as tools of public policy … are not absolute and unlimited but are generally subject to a number of limitations and exceptions that aim to balance the legitimate interest of right holders and users. These limitations and exceptions, together with the carefully defined scope of protectable subject matter and a limited term of protection, are policy instruments so that the system as a whole can be effective in meeting its stated objectives').

[17] M. Burri and M. Vasquez Callo-Müller, 'TAPED: Trade Agreements Provisions on Electronic Commerce and Data', https://unilu.ch/taped (accessed 20 February 2026). TAPED covers all Preferential Trade Agreements from January 2000 to September 2025, including chapters on IP.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

under digital trade rulemaking, beyond the already well-studied area of data-related provisions.[18] By situating source code provisions within the evolution (or relative stagnation) of international IP law, this article makes two contributions. First, it reframes the debate from the question of regulatory chill to the governance implications of regime shift. Second, it shows that exceptions and carve-outs in digital trade chapters in FTAs and DEAs, particularly those at the provision-level, deserve greater attention as they determine the boundaries between source code protection and legitimate public policy disclosure. The relevant question is thus no longer whether source code protection should be included in digital trade rulemaking (as scholars have questioned[19]), but how the mechanisms to allow regulatory oversight over software source code and algorithms should be better structured under digital trade law.

This article is structured as follows: after presenting a necessary overview of the current state of source code provisions in trade agreements, their scope, and the motives behind their inclusion under digital trade law (Section 2), this article analyses the interface between source code provisions and international IP law, focusing on trade secret protection in TRIPS-plus agreements (Section 3). It then examines the source code provision's exceptions and carve-outs, which are of key importance in preserving regulatory autonomy (Section 4). Section 5 concludes.

2. Source Code Regulation in FTAs and DEAs

2.1 Overview

FTAs and DEAs[20] increasingly contain provisions on source code as one of the important issues of the data-driven economy. However, the inclusion of such provisions is still less frequent than the coverage of other pertinent issues, such as cross-border data flows, data localization requirements, and personal data protection.[21] The basic obligation in a source code provision is banning the requirement to transfer or provide access to source code and, if applicable, algorithms. Except for some treaties, which provide for an unconditional and succinct obligation (simply: '[A] Party shall not require the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party'[22]), there will be an explicit reference that the context of this general obligation is when such transfer or access is a condition for market access (including post-import measures, i.e., distribution, sale or use). Typically, parties to an FTA or DEA will agree to the following language:

> [N]ot to require the transfer of, or access to, source code of software owned by a person of the other Party, *as a condition* for the import, distribution, sale or use of such software, or of products containing such software, in its territory [emphasis added].[23]

Some EU FTAs and DEAs differ slightly in the formulation of the basic obligation, stating, in some cases, that requirements to transfer or access to source code shall not apply as a condition for the *export* of that software,[24] potentially expanding the scope of the source code beyond market access. In addition, most treaties also clarify that the 'source code of software owned by a person of the other Party' includes the source code of software contained in a product.[25] By adding the word 'includes',

[18] See generally M. Burri and K. Kugler (2024) 'Regulatory Autonomy in Digital Trade Agreements', *Journal of International Economic Law* 27, 397–423.

[19] Irion, supra n. 10.

[20] See generally M. Burri et al. (2025) 'Understanding Digital Economy Agreements as a New Model of Trade Governance', *Legal Issues of Economic Integration* 52(3), 219–250.

[21] M. Burri et al. (2024) 'The Evolution of Digital Trade Law: Insights from TAPED', *World Trade Review* 23, 190.

[22] See EU–UK TCA, Article 207 (1), and EFTA–Moldova FTA, Article 5.14.

[23] See, for example, Indonesia–Australia CEPA, Article 13.13.

[24] EU–Korea DTA, Article 11. ('[a] condition for the import, *export*, distribution, sale, or use of that software, or of products containing that software, in or from its territory' (emphasis added)). See also EU–New Zealand FTA, Article 12.11 (2) and EU–Singapore DTA, Article 11 (1).

[25] EU–Japan FTA, Article 8.73, footnote 1.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

this provision also applies when software is, for instance, provided as a service or as part of a product, such as in the case of automated vehicles. Notwithstanding the explained differences, FTAs and DEAs share a quite standard basic obligation, complemented by parties agreeing to carve-outs (i.e. to exclude certain measures from the scope of application) as well as exceptions. These carve-outs and exceptions, which relate to the public policy reasons for governments to mandate transfer of, or access to, source code,[26] vary among FTAs and DEAs (see Section 4).

To date, out of the 149 FTAs that have specific chapters on e-commerce or digital trade,[27] only 41 incorporate a relevant provision on source code. The first agreement, which included a provision on source code, was the Japan–Mongolia FTA of 2015. Since then, such a provision has been included in mega-regional agreements, such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States–Mexico–Canada Agreement (USMCA). Moreover, all DEAs contain a provision on the non-disclosure of source code.[28] The only exception is the 2020 Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand, Singapore (and, as of 2024, Korea and, as of 2026, Peru). However, the DEPA parties are independently obliged by binding source code provisions under different treaties.[29] The 2024 AfCFTA Digital Trade Protocol also includes a provision on source code. The scope of this provision, carve-outs, and exceptions is further clarified through a dedicated Annex. The AfCFTA Digital Trade Protocol Annex on 'Criteria for Determining the Legitimate and Legal Public Interest Reasons for Disclosure of Source Code'[30] is one of its kind in articulating the legitimate and legal public interests that might require the disclosure of source code. It also includes safeguards to protect source code in case of eventual disclosure, including measures requiring protection from cybercrimes and cyber threats, an aspect not observed with such a level of detail in other FTAs and DEAs.

It is important to highlight that due to their legal design (namely, the establishment of a prohibition), source code provisions are, to a large extent, binding. The only two agreements not incorporating a binding provision but a commitment for parties to continue dialogue on source code are the Regional Comprehensive Economic Partnership (RCEP)[31] and the 2024 China–Peru Optimization Protocol.[32] In addition, the most recent US agreements with Malaysia,[33] Cambodia,[34]

[26]C. Dorobantu et al. (2021) 'Source Code Disclosure: A Primer for Trade Negotiators', in I. Borchert and A. Winters (eds), *Addressing Impediments to Digital Trade*. CERP Press, 124.

[27]Based on the TAPED dataset (updated until September 2025), supra n. 17.

[28]US–Japan DTA, Article 17; Australia–Singapore DEA, Article 28; UK–Singapore DEA, Article 8.61-K; Korea–Singapore DEA, Article 14.19; UK–Ukraine DTA, Article 132-P; AfCFTA Digital Trade Protocol, Article 24; EU–Singapore DTA, Article 11; EU–Korea DTA, Article 11; EFTA–Singapore DEA, Article 36-P.

[29]See Singapore–Australia DEA, Article 28; Singapore–UK DEA, Article 8.61-K (1); Korea–Singapore DEA, Article 14.19; Singapore New Zealand CEPA (Upgrade), Article 9.13; EU–Chile Interim Agreement, Article 9.12; CPTPP, Article 14.2.

[30]See AfCFTA Source Code Annex, supra n. 4.

[31]See Regional Comprehensive Economic Partnership (RCEP), Article 12.16: Dialogue on Electronic Commerce:

1. The Parties recognise the value of dialogue, including with stakeholders where appropriate, in promoting the development and use of electronic commerce. In conducting such a dialogue, the Parties shall consider the following matters: …

(b) current and emerging issues, such as the treatment of digital products, source code, and cross-border data flow and the location of computing facilities in financial services.

[32]See 'China–Peru Optimization Protocol, Article 18.14: Future Negotiating Clause.

The Parties undertake to initiate discussions to further deepen the electronic commerce commitments including source code and non-discriminatory treatment to digital products, if both parties agree to these disciplines in any trade agreement that is subscribed or enters into force after the entry into force of this agreement.

[33]Agreement between the United States of America and Malaysia on Reciprocal Trade, 26 October 2025 (US–Malaysia Reciprocal Trade Agreement) (see Section 3, Digital Trade and Technology, Article 3.4).

[34]'Agreement between the United States of America and the Kingdom of Cambodia on Reciprocal Trade', 26 October 2025 (US–Cambodia Reciprocal Trade Agreement) (see Section 3, 'Digital Trade and Technology', Article 3.4).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

and Taiwan[35] contain source code provisions under the general umbrella of 'market access' commitments, which is a slightly different formulation that not only covers source code but also expands its scope to cover a particular technology, production process, or other proprietary knowledge.[36]

Thus, the countries and regions with a binding source code provision in at least one FTA or DEA are: the AfCFTA member states, Australia, Canada, Cambodia, Chile, Colombia (as a member of the Pacific Alliance), EFTA member states, the EU, Hong Kong, Iceland, India, Indonesia Japan, Korea, Liechtenstein, Malaysia, Mexico, Moldova, Mongolia, New Zealand, Norway, Paraguay, Peru, Singapore, United Arab Emirates (UAE), Ukraine, United Kingdom (UK), and the US. Absent from this group is notably China, whose alleged policies on forced technology transfer initially drove the inclusion of this provision in trade agreements, as will be explained in the later subsection. China has, thus far, only agreed to maintain dialogue on this issue under RCEP and the Peru–China Optimization Protocol. For a list of all treaties incorporating a source code provision, see Table 1.

2.1.1 Scope of the Non-Disclosure of Source Code Provision

The scope of what is covered by source code is not generally defined in FTAs or DEAs. Because of this lack of a clear definition, there are concerns that source code provisions may create ambiguity that may shield Application Programming Interfaces (APIs),[37] algorithms,[38] and even data used to train algorithms.[39]

In some cases, the source code provision will specifically provide that it extends its coverage to algorithms. For example, the USMCA states that '[n]o Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, *or to an algorithm expressed in that source code*'.[40] A much more detailed and careful language on whether source code encompass algorithms (and only to a certain extent) is included in the Australia–United Arab Emirates (UAE) CEPA, which clarifies that the 'a reference to "source code" includes an algorithm embedded in the source code, *but does not include the expression of the algorithm in any other form, including prose*' (emphasis added).[41] The same clarification is included in the recent India–UK CETA[42] and the UK–Ukraine DTA.[43] Finally, in other treaties, the scope of the source code will be extended to cover algorithms when other agreements covering algorithms are agreed upon by the parties. For instance, Article 28 (5) of the Australia–Singapore DEA provides:

> If both Parties undertake obligations under: (a) an international agreement that enters into force after the date of entry into force of this Agreement; or (b) an amendment to any existing

[35] Agreement between the American Institute in Taiwan and the Taipei Economic and Cultural Representative Office in the United States on Reciprocal Trade between the United States of America and Taiwan, 12 February 2026 (Taiwan–US Reciprocal Trade Agreement).

[36] See Malaysia–US Reciprocal Trade Agreement, Article 3.4.1:

Article 3.4: Market Entry Conditions

1. Malaysia shall not impose any condition or enforce any undertaking requiring US persons to transfer or provide access to a particular technology, production process, source code, or other proprietary knowledge, or to purchase, utilize, or accord a preference to a particular technology, as a condition for doing business in its territory.

[37] Irion, supra n. 10, 1564.

[38] Ibid.

[39] Jones et al., supra n. 10, 13–14 ('Code is often used to refer to computer algorithms and machine learning models as these count as instructions that can be compiled and executed by a computer. As a result, the provision might reasonably be interpreted to include algorithms, training data, datasets, and other related components. This broadens the scope of source code provisions, creating ambiguity about what is truly covered, and poses even greater challenges for the regulation of algorithmic and AI systems.')

[40] See, for example, USMCA, Article 19.16, New Zealand–UK FTA, Article 15.12(1)(a), and Singapore–UK DEA, Article 8.61-K(1).

[41] Australia–UAE CEPA, Article 12.21, footnote 5.

[42] India–UK CEPA, Article 12.15, footnote 9.

[43] UK–Ukraine DTA, Article 132-A.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

Table 1. Source code provisions in trade agreements

Agreement	Year of signature	Source code provision	Algorithms are covered
Japan–Mongolia FTA	2015	x	
Australia–Peru FTA	2018	x	
CPTPP	2018	x	
EU–Japan EPA	2018	x	
USMCA	2018	x	x
Australia–Indonesia CEPA	2019	x	
Australia–Hong Kong FTA	2019	x	
Japan–US DTA	2019	x	x
Singapore–New Zealand CEPA Upgrade	2019	x	
Australia–Singapore DEA	2020	x	x***
RCEP	2020	x*	
Japan–UK CEPA	2020	x	x
EU–UK TCA	2020	x	
Iceland, Liechtenstein, Norway–UK FTA	2021	x	
Chile–Paraguay FTA	2021	x	
Australia–UK FTA	2021	x	x
Pacific Alliance–Singapore FTA	2022	x	x
Singapore–UK DEA	2022	x	x
Korea–Singapore DEA	2022	x	x
EU–New Zealand FTA	2023	x	
EFTA–Moldova FTA	2023	x	
Canada–Ukraine Modernized FTA	2023	x	x
UK–Ukraine DTA	2023	x	x****
AfCFTA Digital Trade Protocol	2024	x	x
Australia–UAE CEPA	2024	x	x****
Chile–UAE CEPA	2024	x	
China–Peru Optimization Protocol	2024	x*	
Hong Kong, China–Peru FTA	2024	x	
EU–Singapore DTA	2025	x	
India–UK CETA	2025	x	x****
EU–Korea DTA	2025	x**	
EFTA–Singapore FTA	2025	x	
EU–Chile AdvancedFramework Agreement	2024	x	
Canada–Indonesia CEPA	2025	x	
EFTA–Ukraine Modernized FTA	2025	x	
EU–Indonesia CEPA	2025	x**	
Cambodia–US Reciprocal TradeAgreement	2025	x	x
Malaysia–US Reciprocal Trade Agreement	2025	x	x

(*Continued*)

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use , available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

Table 1. (*Continued.*)

Agreement	Year of signature	Source code provision	Algorithms are covered
EU–Mexico Modernized Agreement	2025	x**	
EU–India FTA	2026	x**	
US–Taiwan Agreement on ReciprocalTrade	2026	x	x

Notes:
*Only provision committing to maintain dialogue.
**According to the textual proposal.
***Conditional to future agreement.
****Further clarifying that a reference to 'source code' includes an algorithm embedded in the source code, but does not include the expression of the algorithm in any other form, including prose.
Source: Author's elaboration based on TAPED.

> international agreement, to not require the transfer of, or access to, an algorithm expressed in source code of software owned by a person of a Party or non-Party as a condition for the import, distribution, sale or use of that software, or of products containing that software, in their respective territories, this Article shall apply, mutatis mutandis, to algorithms expressed in source code of software owned by a person of the other Party.

These different ways to explicitly include algorithms, or foresee the expansion of the scope of the source code provision to cover these, indicate that governments negotiate this provision under the understanding that only by explicitly including 'algorithms' does the source code provision apply to these, and only to the extent stated in those provisions. An extension of the scope of the source code provision to cover algorithms is particularly important for AI, as some AI algorithms are not source code and may, therefore, be excluded from protection.[44]

To further buttress the difference between 'source code' and 'algorithms', one can seek to define the ordinary meanings of both terms. Although Article 31 of the Vienna Convention of the Law of Treaties (VCLT)[45] does not require the use of dictionaries, tribunals frequently refer to dictionary definitions as a means of identifying the ordinary meaning of treaty terms.[46] In light of this practice, the dictionary definition of source code is the following: '[a] text listing of commands to be compiled or assembled into an executable computer program'.[47] 'Algorithms', in contrast, are defined more broadly as '[a] process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer'.[48]

Against this background, none of the current FTAs and DEAs, except for the AfCFTA Annex on Source Code, contains a definition of source code. The relevant AfCFTA Annex defines source code as a 'set of programmed instructions written by a programmer using a specific programming language to execute or perform particular tasks or functions, which is typically a human-readable version and can be executed by a computer to form the foundation of a software'.[49] In the same Annex, algorithms are defined as '[a] defined set of digital sequential procedures, used to solve a particular problem,

[44] J. Ferencz et al. (2022) 'Artificial Intelligence and International Trade: Some Preliminary Implications', OECD Trade Policy Paper No. 260, 21.

[45] Article 31.1 Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331 (VCLT) Article 31(1). ('A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.')

[46] Chang-Fa Lo (2010) 'Good Faith Use of Dictionary in the Search of Ordinary Meaning under the WTO Dispute Settlement Understanding', *Journal of International Dispute Settlement* 1, 431; I. Van Damme (2011) 'On "Good Faith Use of Dictionary in the Search of Ordinary Meaning under the WTO Dispute Settlement Understanding" – A Reply to Professor Chang-Fa Lo', *Journal of International Dispute Settlement* 2, 231.

[47] A. Stevenson (ed.) (2010) *Oxford Dictionary of English*. Oxford University Press.

[48] Ibid.

[49] AfCFTA Source Code Annex, Article 1(c).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

or execute or perform a particular task',[50] a much broader and encompassing definition than the respective source code one. These definitions closely follow the dictionary definitions of both terms.[51]

Technically, however, a clear differentiation between source code and algorithms is more nuanced, as there are some overlaps between both notions. Algorithms can be manifested in source code (such as in hand-coded algorithms),[52] and those will be covered when an FTA or DEA states that the source code provision encompasses an algorithm expressed in that source code. In other cases, algorithms will evolve (the so-called non-deterministic or learning algorithms) and are thus 'not limited to the commands in the program code but evolve through the influence of non-predictable elements'.[53] This second category goes beyond the current scope of protection of source code provisions in FTAs and DEAs. The conundrum to differentiate between source code and algorithms is not only present in digital trade law but also in philosophy[54] and computer science.[55] This lack of clarity also affects the understanding of algorithms in public discourse, with evident ramifications in their inclusion in international trade negotiations. As noted by Mittelstadt et al., '[R]eferences to algorithms in public discourse do not normally address algorithms as mathematical constructs, but rather particular implementations. Lay usage of "algorithm" also includes implementation of the mathematical construct into a technology and an application of the technology configured for a particular task.'[56]

However, the manner in which 'source code' and 'algorithms' have been incorporated into trade agreements (explicit incorporation, incorporation by that have specific chapters on e-commerce source code encompasses algorithms and to what extent) points to an intentional differentiation between these two subject matters. Provisions in current FTAs and DEAs that refer only to source code, therefore apply only to that subject matter and do not automatically extend to algorithms, which otherwise would have significant regulatory consequences.[57] A notable evolution in the incorporation of source code provisions from FTAs to DEAs further exemplifies this. DEAs, excluding the case of EU Digital Trade Agreements (DTAs) and EFTA DEAs, expand the scope of the source code provision to cover algorithms. Explicit reference to 'algorithms' appears in the US–Japan DTA,[58] the UK–Singapore DEA,[59] the Korea–Singapore DEA,[60] the UK–Ukraine DTA,[61] and the AfCFTA Digital Trade Protocol.[62] In the case of the Australia–Singapore DEA, the parties agreed to expand the scope of the source code provision to cover algorithms when other FTAs covering algorithms will be agreed upon by the parties.[63] Notably, EU DTAs omit any reference to 'algorithms', limiting the scope of the source code provisions to the software's source code only, thus preserving policy space for regulatory measures that might imply access to algorithms, such as those included in the EU AI Act.[64] This choice is consistent across EU FTAs and DEAs.[65]

[50] AfCFTA Source Code Annex, Article 1(a).

[51] See, supra n. 47 and n. 48.

[52] Irion, supra 10, 1564.

[53] P. Picht et al. (2024) 'New Software Protection Approaches in a World (Co)Shaped by AI', Swiss Federal Institute of Intellectual Property, 13, 7.

[54] B.D. Mittelstadt et al. (2016) 'The Ethics of Algorithms: Mapping the Debate', *Big Data & Society* 3, 2; See also R.K. Hill (2016) 'What an Algorithm Is', *Philosophy and Technology* 29, 35.

[55] M.Y. Vardi (2012) 'What Is an Algorithm?', *Communications of the AMC* 55, 5.

[56] Mittelstadt et al., supra n. 54, 2.

[57] See generally K. Yeung (2018) 'Algorithmic Regulation: A Critical Interrogation', *Regulation & Governance* 12, 505.

[58] US–Japan DTA, Article 17 (1).

[59] UK–Singapore DEA, Article 8.61-K (1).

[60] Korea–Singapore DEA, Article 14.19 (1).

[61] UK–Ukraine DTA, Article 132-P (1), footnote 9.

[62] AfCFTA Digital Trade Protocol, Article 24 (1).

[63] Australia–Singapore DEA, Article 28 (4).

[64] EU AI Act, Article 74.

[65] See Article 11 of EU DTAs with Korea and Singapore vis-à-vis Article 12.11 of EU–New Zealand FTA.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

3. Objectives of Source Code Provisions in Digital Trade Law and IP Overlaps

In general, the emergence of source code provisions in digital trade rulemaking has been associated with the risks of forced technology transfer,[66] most prominently exemplified by the US–China trade frictions,[67] whereby tech companies were allegedly required to transfer source code, and hence, their technology, as a precondition to operate in the Chinese market. These technology transfer requirements are included in some of China's regulations (in particular, the Cybersecurity Law and related guidelines[68]) and have been raised as an issue in the 2017 US Section 301 report.[69] More recently, force technology transfer concerns have been reiterated in the 2025 US National Trade Estimates Report.[70] In addition, the Trump administration has also highlighted its concerns regarding the EU AI Act, particularly relating to the requirements affecting 'source code, trade secrets, and copyright protection'.[71] Some academic studies show that certain African countries, specifically Nigeria and South Africa, also require the mandatory disclosure of source code; however, these are for different reasons. In the case of Nigeria, disclosure of source code is required for security purposes, while in the case of South Africa, disclosure is required when the software is used by the government.[72]

Beyond the case of China and the fear of forced technology transfer, it can be argued that source code provisions on FTAs and DEAs are also a mechanism to shield sensitive proprietary information from the risks of disclosure during administrative procedures, including licensing, certification, and conformity assessment.[73] These can entail the loss of secrecy of confidential information, and hence of its commercial value. This is evident from the evolving language in these provisions, which in a few instances refer specifically to trade secret protection.[74] It is also most recently exemplified by the EFTA–Singapore DEA, which specifically mentions the protection of trade secrets as one of the objectives of the treaty,[75] while also incorporating a provision on source code.[76]

The growing reference to trade secrets in the digital trade discourse is a much lesser explored aspect in the debate regarding source code, but it is key in understanding why source code provisions exist at all in digital trade, as they are a functional response to the inadequacy of the international IP system to protect software and algorithms, as analyzed in the next section.

[66] T.H. Moran (2015) 'Should US Tech Companies Share Their "Source Code" with China?', *China Economic Watch*, 28 October 2015, www.piie.com/blogs/china-economic-watch/should-us-tech-companies-share-their-source-code-china (accessed 11 April 2025).

[67] See generally J.Y. Qin (2019), 'Forced Technology Transfer and the US–China Trade War: Implications for International Economic Law', *Journal of International Economic Law* 22, 743.

[68] See J. Hsu (2015) 'China's New Rules Ask Tech Firms to Hand Over Source Code', *IEEE Spectrum*. See also M. Parasol (2018) 'The Impact of China's 2016 Cyber Security Law on Foreign Technology Firms, and on China's Big Data and Smart City Dreams', *Computer Law & Security Review* 34, 67.

[69] USTR, 'Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974', 22 March 2018, 43, https://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-china/investigation (accessed 11 April 2025).

[70] USTR, '2025 National Trade Estimate Report on Foreign Trade Barriers of the President of the United States on the Trade Agreements Program', 31 March 2025, 72, https://ustr.gov/about/policy-offices/press-office/press-releases/2025/march/ustr-releases-2025-national-trade-estimate-report (accessed 11 April 2025).

[71] Ibid, at 147.

[72] R. Tavengerwei et al. (2022) 'What to Consider Ahead of the AfCFTA Phase II Negotiations: Focus on Digital Trade Policy Issues in Four Sub-Saharan African Countries', 3.

[73] Andrenelli et al., supra n. 14, 8

[74] See Australia–Singapore DEA, Article 28, footnote 14.

[75] EFTA–Singapore DEA, Article 36-C(c)(ii) ('The Parties seek to: (c) create an environment of trust and confidence in, as well as security for digital trade, including through: (ii) the protection of trade secrets.')

[76] EFTA–Singapore DEA, Article 36-P.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

3.1 IP and the Protection of Software and Algorithms

Theoretically, different IP rights are available for the protection of software's source code and algorithms, primarily copyright, patents, and trade secrets. The protection of software and computer programs' source code as a copyrighted works under the TRIPS Agreement is recognized in TRIPS Article 10 (on 'Computer programs and compilations of data'). Before TRIPS, it was generally understood that computer programs were protected by copyright, but differences existed among jurisdictions. After failed attempts for a WIPO Treaty on Computer Programs,[77] the explicit protection of computer programs via the TRIPS agreement harmonized the protection for this subject matter to a considerable extent. TRIPS Article 10 provides that 'Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971)'. Article 4 of the WIPO Copyright Treaty[78] reaffirms this by providing that copyright protection applies to computer programs, 'whatever their mode or form of expression'.

According to commentators, the emphasis on source code (instead, among others, algorithms) was an aspect explicitly deliberated in TRIPS discussions.[79] Other commentators, however, note that the scope of this provision 'could be considered as (covering) the whole realm of manifestations of computer programs'.[80] Accordingly, it should 'be interpreted as covering other forms of expression (that is, programming) that may emerge and that would make this distinction between source and object code obsolete'.[81] However, it is unclear if this would imply the protection of algorithms, particularly considering that Article 9.2 of TRIPS provides that '[C]opyright protection shall extend to expressions and not to ideas, methods of operation or mathematical concepts *as such*' (emphasis added). Following this, TRIPS would not cover algorithms under copyright protection, as they are primarily mathematical constructs. The EU Directive on the Legal Protection of Computer Programs[82] provides further clarification on how domestic laws have implemented Article 10 of the TRIPS Agreement in the sense that algorithms are not implicitly covered by the term 'source code'. It clarifies that:

> For the avoidance of doubt, it has to be made clear that only the expression of a computer program is protected and that ideas and principles which underlie any element of a program, including those which underlie its interfaces, are not protected by copyright under this Directive. In accordance with this principle of copyright, to the extent that logic, *algorithms* and programming languages comprise ideas and principles, those ideas and principles are not protected under this Directive.'[83] (Emphasis added)

Case law arising from the Court of Justice of the European Union (CJEU) also showcases a strict interpretation of the scope of the Computer Programs Directive, limiting its application to software source code.[84] As things stand, what is protected under the EU Directive is the code or structure of a computer program, but not the algorithms themselves.[85] Legal scholars explain the underlying logic

[77] WIPO (1983) 'Legal Protection of Computer Software', *Journal of World Trade* 17, 537.

[78] WIPO Copyright Treaty (adopted 20 December 1996, entered into force 6 March 2002), 2186 UNTS 121.

[79] See generally T. Dreier (1989), 'National Treatment, Reciprocity and Retorsion – The Case of Computer Programs and Integrated Circuits', in F.-K. Beier and G. Schricker (eds), *GATT or WIPO? The New Ways in the International Protection of Intellectual Property*, vol 11. VCH Publishers.

[80] D. Gervais (2021) *The TRIPS Agreement: Drafting History and Analysis,* 5th edn. Sweet & Maxwell, 3.166.

[81] Ibid.

[82] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L 111, 5.5.2009, pp. 16–22.

[83] Ibid, recital 11.

[84] Case C-393/09 Bezpečnostní softwarová asociace – Svaz softwarové ochrany v Ministerstvo kultury ECLI:EU:C:2010:816, para. 42 ('It follows that that interface does not constitute a form of expression of a computer program within the meaning of Article 1(2) of Directive 91/250 and that, consequently, it cannot be protected specifically by copyright in computer programs by virtue of that directive.')

[85] See also B. Gonzalez Otero (2021) 'Machine Learning Models under the Copyright Microscope: Is EU Copyright Fit for Purpose?', *GRUR International* 70, 1043, 1053.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

clearly, noting that copyright 'focus[es] on the code layer of the computer program … allowing to think of them as linguistic works'.[86] By emphasizing this 'linguistic approach', algorithms, as such, are not protected under copyright law.[87]

Another avenue for potential protection is patent law. While Article 27 of the TRIPS Agreement (on 'Patentable subject matter') does not exclude a priori software source code or algorithms, software-related inventions will only be protected if the requirements of technical nature, inventive step, and non-obviousness are met.[88] Furthermore, in some jurisdictions, patent offices exclude mathematical methods (which include algorithms) and computer programs from patentability.[89] This does not mean that AI-related inventions (part of the wider category of Computer Implemented Inventions) cannot be patentable, but it has to be demonstrated that they serve a technical effect beyond their implementation on a computer.[90] Moreover, to be protected, AI-related inventions must be sufficiently disclosed so that the person skilled in the art can implement them.[91] This knowledge will later enter the public domain. This disclosure – or 'patent bargain' – is a necessary precondition of the patent system. While this could seem at odds with the need to protect sensitive information in source code and algorithms (for instance, as evident from the drive to include source provisions in FTAs and DEAs), it did not, in practice, dissuade inventors from filling AI-related inventions. According to the WIPO Patent Landscape Report, AI-related inventions are on the rise, with an even sharper increase after the wider diffusion of Generative AI.[92] Despite all this, and because of the requirements for patentability and thresholds that should be met, there have been consistent doubts about the feasibility of protecting source code and algorithms under patent law,[93] which leads to favor protection under trade secret law.[94]

Indeed, the law of undisclosed information (or trade secrets), codified in Article 39 of the TRIPS agreement, remains another avenue for potential protection. Under TRIPS Article 39, undisclosed information is protected if three conditions are met: the information is secret, has commercial value because of its secrecy, and has been subject to reasonable steps to keep it secret. These requirements form the international threshold of protection. This threshold of protection does not assess the quality or inherent characteristics of the subject matter of protection – such as whether it is inventive, which is one of the thresholds for patent protection, or original, a key requirement for protection under

[86] Pitch et al., supra n. 53, 28.

[87] Ibid, 29.

[88] Article 27 TRIPS on Patentable Subject Matter ('1. Subject to the provisions of paragraphs 2 and 3, patents shall be available for any inventions, whether products or processes, in all fields of technology, provided that they are new, involve an inventive step and are capable of industrial application').

[89] European Patent Office (EPO), *European Patent Convention*, Article 52 (2)(a) ('Patentable inventions: (1) European patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application. (2) The following in particular shall not be regarded as inventions within the meaning of paragraph 1: (a) discoveries, scientific theories and *mathematical methods*' (emphasis added)). However, for mathematical methods to be patentable, they must have a technical character. See EPO, Guidelines for Examination in the European Patent Office, section 3.3.1: Artificial Intelligence and Machine Learning (highlighting that AI and Machine learning, to be patented, needs to contribute to the technical character of the invention).

[90] Ibid, EPO, Guidelines for Examination in the European Patent Office.

[91] TRIPS, Article 29.1 (on 'Conditions on Patent Applicants'). See also: WIPO (2023) 'WIPO Patent Drafting Manual', 27, www.wipo.int/edocs/pubdocs/en/wipo-pub-867-23-en-wipo-patent-drafting-manual.pdf (accessed 11 April 2025).

[92] WIPO (2024) 'Patent Landscape Report: Generative Artificial Intelligence' 34, www.wipo.int/web-publications/patent-landscape-report-generative-artificial-intelligence-genai/en/index.html (accessed 11 April 2025).

[93] The debate on the patentability of software is not new, and it certainly does not belong exclusively to the EU. In the US, the patentability of software is a debated issue as well. See J. Saltiel (2019) 'Five Years after Alice: Five Lessons Learned from the Treatment of Software Patents in Litigation', WIPO Magazine, www.wipo.int/web/wipo-magazine/article-details/?assetRef=40932&title=in-the-courts-five-years-after-alice-five-lessons-learned-from-the-treatment-of-software-patents-in-litigation (accessed 12 April 2025). See also: N. Shemtov (2017) *Beyond the Code: Protection of Non-Textual Features of Software*, 1st edn. Oxford University Press.

[94] See K. Foss-Solbrekk (2021) 'Three Routes to Protecting AI Systems and Their Algorithms under IP Law: The Good, the Bad and the Ugly', *Journal of Intellectual Property Law and Practice* 16, 247, 253–256.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

copyright law. In this respect, IP scholars have often noted that trade secrets offer a more viable legal vehicle to protect source code and algorithms than patent law,[95] for better or for worse.[96]

At this point, a clarification is warranted. Article 39.2 of the TRIPS Agreement, which deals with trade secrets, details that '[n]atural and legal persons shall have the *"possibility"* of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices' (emphasis added). The textual interpretation of this provision does not denote a compelling obligation to protect trade secrets. By using the word 'possibility', the provision sets a 'low bar' for WTO members,[97] which has allowed them to protect undisclosed information without the need to implement specific legislation, as some already count with unfair competition laws.[98] This also explains why major jurisdictions enacted specific laws for trade secret protection in only in the past few years and not right after TRIPS was adopted. Only in 2016 did the US adopt the Defend Trade Secrets Act,[99] establishing federal civil protection for trade secrets, while the EU adopted its Trade Secrets Directive the same year.[100]

More importantly, there is a key difference between the scope of protection of software's source code and algorithms through digital trade law vis-à-vis trade secret protection under TRIPS. Namely, the scope of protection that Article 39.2 of TRIPS offers is limited to the breach of confidence contrary to honest commercial practices. The term 'commercial practices' refers to practices undertaken in the course of 'commerce, trading',[101] applying only within a commercial relationship, which is confirmed if we situate TRIPS Article 39.2 within its original context, namely the notion of 'unfair competition' included in Article 10bis of the Paris Convention.[102] Ricketson notes that according to Article 10bis(a) of the Paris Convention: '[an act of competition] "must be an act of competition … in industrial and commercial matters". This suggests that all that is excluded here are acts of a private, individual or non-commercial kind.'[103] Accordingly, non-commercial practices that would involve a state (for instance, regulatory disclosures or audits) are not considered within the scope of protection. Other state-sponsored practices of a non-commercial nature would also not be covered, for instance state-sponsored misappropriation. A prerequisite for including these practices within the scope of protection of TRIPS Article 39.2 is the existence of a competitive relationship between the entity that is subject to the theft of trade secrets and the entity carrying out the unlawful acquisition. Hence, the need for separate and dedicated legislation in this area.

Furthermore, Article 39.2 of TRIPS does not offer general protection for information submitted to the government. Securing the confidentiality of trade secrets during regulatory or administrative proceedings, especially if the subject matter of protection is not test data, is an aspect that falls beyond the scope of the TRIPS Agreement. The nearest regime is indeed the one provided by Article 39.3 of

[95]T. Aplin (2017) 'Trading Data in the Digital Economy: Trade Secrets Perspective', in S. Lohsse, R. Schulze, and D. Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools: Münster Colloquia on EU Law and the Digital Economy III*, 1st edn. Nomos Verlagsgesellschaft mbH & Co KG.

[96]For a critical view of the use of trade secrets as a mechanism to protect source code, see S.K. Katyal (2019) 'The Paradox of Source Code Secrecy', *Cornell Law Review* 104, 1183.

[97]T. Aplin, L. Bentley, et al. (2012) *Gurry on Breach of Confidence: The Protection of Confidential Information*, 2nd edn. Oxford University Press, 800.

[98]For instance, Japan protects trade secrets under Article 2 of its 1993 Unfair Competition Prevention Act. See Japan, Unfair Competition Prevention Act (Act No. 47 of 19 May 1993, as amended up to Act No. 75 of 29 June 2005).

[99]US, Defend Trade Secrets Act of 2016, Public Law No. 114–153.

[100]Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure OJ L 157, 15.6.2016, pp. 1–18, EU Trade Secrets Directive.

[101]A. Stevenson (ed.) (2010) *Oxford Dictionary of English*. Oxford University Press.

[102]Article 10bis Paris Convention for the Protection of Industrial Property, opened for signature 20 March 1883, revised at Stockholm, 14 July 1967, 828 UNTS 305, as amended on 28 September 1979 (entered into force 3 June 1984) (Paris Convention), incorporated by reference in Article 39(1) of the TRIPS Agreement.

[103]S. Ricketson (2015) *The Paris Convention for the Protection of Industrial Property: A Commentary*. Oxford University Press, para. 13.47.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

TRIPS, which is only applicable to data used to obtain marketing authorization for new chemical entities clinical trial data). The legislative history of this provision shows how its scope of application was narrowed down to cover only clinical trial datasets for 'pharmaceutical or agricultural chemical products'. This occurred despite the initial language proposed by the US and Switzerland for the 'protection of trade secrets submitted to governments without any discrimination as to the field of technology'.[104] The narrowing of the scope of application of TRIPS Article 39.3 occurred at the Brussels Conference held in July 1990, making evident that the intention was to establish a sui generis regime applicable only to pharmaceutical and agricultural chemical products. As a result, no part of the TRIPS Agreement requires WTO members to protect trade secrets that have been submitted to governmental entities, except for the obligations regarding the protection of regulatory test data.[105] Due to these gaps in protection, and because TRIPS only establishes minimum levels of protection, domestic legislation has advanced to provide increased protection when confidential information is submitted to the government. The EU AI Act, for instance, contains the obligation to maintain the confidentiality of the trade secrets submitted to the EU Commission, market surveillance authorities, and notified bodies,[106] going evidently beyond TRIPS minimum standards, notwithstanding the exceptions under the Trade Secrets Directive.[107] However, the protection of trade secret protection internationally remains uneven.

As a result, digital trade law fills the gaps identified in the current IP regime by establishing an *ex-ante* layer of protection for source code and algorithms, and, if software's source code or algorithms qualify for protection via IP, particularly through trade secrets, it also acts as an *additional layer* of protection.

3.1.1 Digital Trade Law as an Ex-Ante Layer of Protection for Source Code and Algorithms

As an ex-ante layer of protection, digital trade affords a key benefit for protecting software's source code – that is, such protection will not depend on the legal requirements to qualify as protected subject matter under copyright, patents, or trade secrets. In this sense, digital trade provisions on the non-disclosure of source code provide a preemptive protection – namely, a ban. As explained earlier, depending on the specific language of each treaty, algorithms may also be covered under the scope of these provisions, solving the conundrum of finding suitable IP rights to protect algorithms. This preemptive protection is even more important for protecting the latter, as it could constitute a *sui generis* protection for this subject matter.[108] *Sui generis* rights, such as the one established in TRIPS Article 39.3 (on the protection of clinical trial data), arise when the special forms of IP protection cannot adequately protect certain subject matter.[109] Recent studies have concluded that, in light of the inadequacy of the current IP system, as well as the needs of the software industry, there actually might be a need for the establishment of a sui generis 'software right' at the domestic and, eventually, international level.[110]

Indeed, while the source code of software may be protected under copyright law, algorithms remain a contested subject matter of protection under copyright and patent law. The only immediate

[104]N. Pires de Carvalho (2008) *The TRIPS Regime of Antitrust and Undisclosed Information.* Kluwer Law International, para. 39.3.77.

[105]S.K. Sandeen and E.A. Rowe (2018) *Trade Secret Law Including the Defend Trade Secrets Act of 2016 in a Nutshell,* 2nd edn. West Academic Publishing, 341.

[106]EU AI Act, Article 78.

[107]EU Trade Secrets Directive, Article 5. See also U.-M. Mylly (2023) 'Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information', *International Review of Intellectual Property and Competition Law (ICC)* 54, 1013, 1026–1027.

[108]Some scholars have already advocated for the establishment of a sui generis right to protect software in the age AI, mostly grounded on the inadequacy of the current IP system. See Pitch et al., supra n. 53.

[109]See I. Kazeeva (2024) *Sui Generis Intellectual Property Protection: Comparison of EU and US Regulatory Approaches.* Springer, 4–6.

[110]Picht et al., supra n. 53, 56–69.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use , available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

IP available to them is trade secret protection. However, even in this case, the requirements for trade secret protection should be met. For instance, to qualify as a trade secret, the information should be secret, that is, not 'generally known' or 'readily accessible'.[111] The application of this requirement will differ according to each case. If some part of the algorithm has been disclosed, and relevant information may already be available, the requirement of secrecy can be called into question. What often seems to be forgotten is that factual secrecy of information[112] does not equate to legal secrecy under IP law. Furthermore, as discussed previously, trade secret protection only offers imperfect protection because it does not protect confidential information submitted to the government.

Some trade agreements have gone further than TRIPS in this regard, but these are only a few and primarily reflect the concerns of the US. Most prominently, although the US is not a Party to the CPTPP, its imprint is recognizable in the CPTPP trade secret provision. Article 18.78 of the CPTPP (on trade secrets) extends its scope to cover state-owned enterprises (SOEs) as potential subjects of liability for trade secret misappropriation.[113] This extension signifies a shift in the normative scope of trade secret law to cover state-level misappropriation. Significantly, the CPTPP provides, for the first time among FTAs, for criminal procedures for trade secret misappropriation and allows parties to limit the availability of criminal procedures and penalties to specific circumstances.[114] These circumstances appear to clarify which practices are considered unfair competition, an aspect that was left undefined in the Paris Convention. Moreover, they do not merely refer to acts of unfair competition between private actors, but also to acts of unfair competition that affect states. This is evident if one pays attention to CPTPP Article 18.78(3)(e), which refers to acts that are detrimental to a Party's 'economic interests, international relations, or national defence or national security'. The USMCA similarly clarifies that the misappropriation of trade secrets extends to unlawful acts by SOEs.[115] Furthermore, the USMCA introduces a novel prohibition that prevents government officials from disclosing trade secrets outside their official duties in civil, criminal, and regulatory proceedings. It further obliges parties to impose effective deterrents, including fines, employment sanctions, and imprisonment, where such conduct occurs.[116]

In contrast to the above-mentioned treaties, RCEP contains a succinct provision on trade secret protection which provides that: '1. Each Party shall provide protection of undisclosed information in accordance with paragraph 2 of Article 39 of the TRIPS Agreement.'[117] The treatment of trade secret protection in FTAs from other regions tends to be similarly limited. For instance, the Protocol to the Agreement Establishing the African Continental Free Trade Area on Intellectual Property Rights (AfCFTA IP Protocol),[118] echoes TRIPS language and further clarifies that trade secret protection 'shall in no way prejudice the right of a State Party to provide exceptions and limitations to the protection of undisclosed information and related rights … *in line with their developmental interests and priorities*'[119] (emphasis added). These examples showcase, overall, a patchy and insufficient landscape for trade secret protection internationally, which naturally led to considering digital trade law as a more effective venue to protect software source code and, if applicable, algorithms.

[111] TRIPS Agreement, Article 39 (2) (a).

[112] For case studies and a detailed analysis, see: S.K. Sandeen and T. Aplin (2022) 'Trade Secrecy, Factual Secrecy and the Hype Surrounding AI', in R. Abbot (ed.), *Research Handbook on Intellectual Property and Artificial Intelligence*. Edward Elgar Publishing.

[113] CPTPP, Article 18.78(1).

[114] CPTPP, Article 18(78)(3).

[115] USMCA, Article 20 (69).

[116] USMCA, Article 20 (77).

[117] RCEP, Article 11(56).

[118] 'Protocol to the Agreement Establishing the African Continental Free Trade Area on Intellectual Property Rights [AfCFTA IP Protocol]' (adopted on 19 February 2023).

[119] AfCFTA IP Protocol, Article 15(2).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

3.2 Digital Trade Law as an Additional Layer of Protection for Source Code and Algorithms

As an additional layer of protection, the protection of software source code via digital trade fits well into the policy of some countries to protect technological sectors from forced technological transfer.[120] Much of this discourse has been advanced by the US, but it has also been of great concern among other developed nations,[121] although the pendulum is starting to swing in the other direction, as exemplified by the EU considering requiring technology transfer for certain Chinese investments.[122] However, within the initial forced technology transfer discourse, the protection of trade secrets played a key role.[123] In fact, the US–China Phase One Agreement, which was adopted during the first Trump administration, included the enhancement of measures protecting trade secrets in its first article.[124] While no other US FTA IP chapter replicates the same level of detail as the US–China Phase One Agreement, the US remains the main force behind the advancement of the level of protection of trade secrets beyond TRIPS standards, which is crucial for software developers, considering the minimum level of protection provided by TRIPS Article 39.2.

Other international efforts by the US did not, however, result in binding legal commitments. Initiatives to advance the protection of trade secrets in international bodies, such as the WTO (via the 'Friends of Trade Secrets'[125]) or APEC (via the 'Best Practices in Trade Secret Protection and Enforcement Against Misappropriation'[126]) precede the US–Phase One Agreement but also aim in this direction – curving forced technological transfer and protecting sensitive information. Yet they remain non-binding.

In this context, while much of the literature studying the development of TRIPS-Plus provisions has been critical of the above-mentioned developments (with very few exceptions[127]), based on the data gathered in the TAPED dataset, such critiques do not hold when it comes to trade secret protection in FTAs, which remains limited. Figure 1 (below) shows the relatively few agreements containing dedicated trade secret provisions vis-à-vis all the agreements containing IP chapters. As is evident, only a small number of FTAs regulate trade secrets.

Considering the little advancement for trade secret protection internationally, the additional level of protection that digital trade provides for the protection of software source code and, more importantly, for algorithms can be better justified. Yet this justificatory logic is largely absent from the existing literature, which has tended to assess source code provisions primarily through the lens of regulatory constraint imposed by digital trade provisions. This also illustrates how the protection of typical IPish matter (not only data-related issues but also algorithms) will be increasingly pursued through digital trade instruments rather than through the politically demanding process of revising IP disciplines.[128] This choice of forum has systemic consequences. It signals a domain shift in which

[120] Qin, supra n. 67, 745.

[121] WTO, *China – Certain Measures on the Transfer of Technology*, DS549.

[122] 'EU to Demand Technology Transfers from Chinese Companies', *Financial Times*, 18 November 2024.

[123] Qin, supra n. 67, 745.

[124] Article 1, US–China Phase One Agreement. See also P. Nath Upreti and M. Vásquez Callo-Müller (2020) 'Phase One US–China Trade Deal: What Does It Mean for Intellectual Property?', *GRUR International* 69, 389.

[125] A. Merelle Ward (2017) 'How Far Away Is Global Trade Secrets Protection? US Industry's Call to Action as EUIPO Analyzes Baseline Data', *The IPKat*, 15 November 2017), http://ipkitten.blogspot.com/2017/11/how-far-away-is-global-trade-secrets.html (accessed 11 April 2025).

[126] APEC (2016) 'Best Practices in Trade Secret Protection and Enforcement against Misappropriation', https://ustr.gov/sites/default/files/11202016-US-Best-Practices-Trade-Secrets.pdf (accessed 11 April 2025).

[127] M. Trimble (2021) 'Unjustly Vilified TRIPS-Plus?: Intellectual Property Law in Free Trade Agreements', A*merican University Law Review* 71, 1449; M. Burri and M. Vásquez Callo-Müller (2024) 'Charting the Course: Trips-Plus Agreements and the Intersection of Intellectual Property with Digital Trade', *American University Law Review* 73.

[128] See generally: S.K. Sell (2014) 'The Dynamics of International IP Policymaking', in D. Gervais (ed.), *Intellectual Property, Trade and Development.* Oxford University Press.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

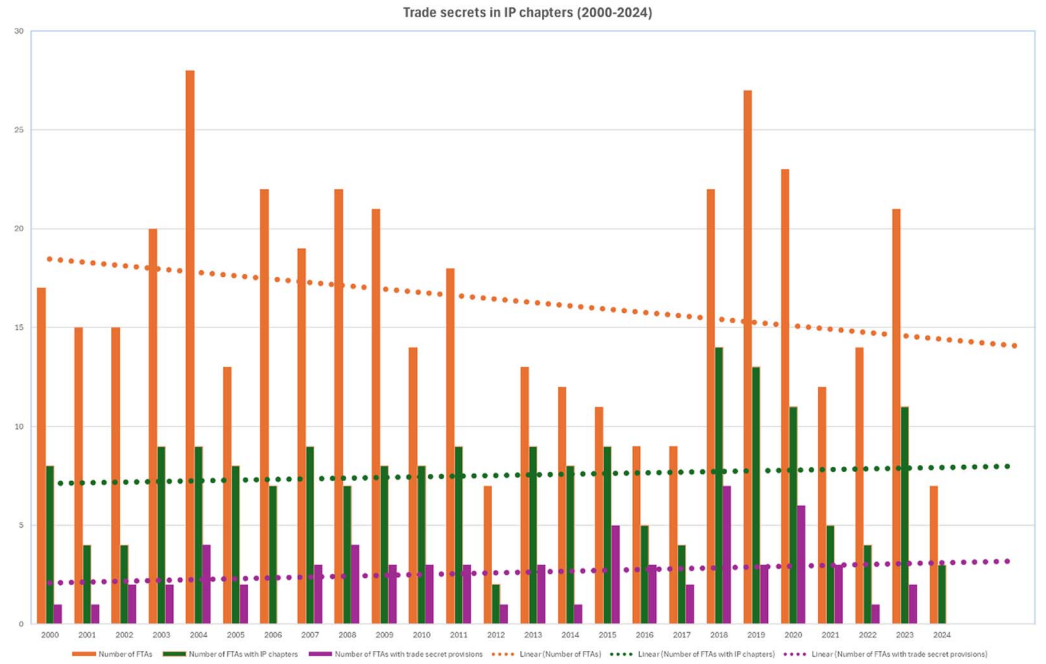


Figure 1. Frequency of trade secret provisions in PTAs (years 2000–2024).
Source: Author's elaboration, based on TAPED.

digital trade law becomes the principal site for the international governance of code and algorithms, while the IP regime remains comparatively static. If it were not for the carve-outs and exceptions to the source code provisions,[129] this would reinforce the critics' fears that only the interests of software and AI providers, but not those of the public at large, are protected. The next subsection discusses those carve-outs and exceptions in detail.

4. Offsetting the Risks of Non-Disclosure of Source Code Provisions in Digital Trade Law

As mentioned in the first part of this Article, a cornerstone of the international IP system is that it is a system built upon the premise of 'balance of rights and obligations', as Article 7 of the TRIPS Agreement indicates.[130] Such a balance is achieved, among others, through the boundaries of the protected subject matter.[131] However, by effectively leaving the realm of IP to regulate the protection of software and algorithms, there is a risk that source code provisions in digital trade rulemaking are cementing rights (that is, protection) without necessary obligations (that is, disclosure). In this context, the regulatory space that source code provisions allow is of key importance in balancing protection and disclosure, and it will determine governments' capacity to regulate software and, in some cases, algorithms, and AI.

[129] See section 2.3.

[130] TRIPS, Article 7 ('[T]he protection and enforcement of intellectual property rights should contribute to the promotion of technological innovation and to the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a *balance of rights and obligations*.') (emphasis added).

[131] Taubmann et al., supra n. 16.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

4.1 Digital Trade Layered Architecture for Regulatory Safeguards

Regulatory space in international trade agreements is safeguarded through various mechanisms, including carve-outs, exceptions, review clauses, and special and differential treatment provisions.[132] In the specific context of digital trade rulemaking, and particularly cross-border data flows, these safeguards have been prominently studied, showcasing the layered way in which they are applied.[133] Consistent with the literature, a further example of how this layering process is occurring is observable in the case of source code provisions. Here too, these tools are being included at least two levels: the 'chapter level' and at the 'provision level'.

At the chapter level, carve-outs and exceptions apply horizontally to all digital trade provisions, including source code, unless otherwise stated, and they often exhibit a high degree of standardization. For instance, according to the TAPED dataset of the 149 FTAs (including DEAs) that incorporate e-commerce or digital trade chapters, about 85% contain security exceptions while about 83% contain general exceptions, sometimes modeled after the general exceptions corresponding to Article XIV of the General Agreement on Trade in Services (GATS)[134] and Article XX of the General Agreement on Tariffs and Trade 1994 (GATT 1994).[135] In the case of carve-outs, government procurement is excluded in 44% of digital trade chapters, while audiovisual services are carved out in about 11% of digital trade chapters and financial services in about 5%.[136]

Despite the prevalence of some of those safeguards, such as general and security exceptions, which are included in most of the FTAs with digital trade chapters, their functional limits have been questioned when applied to the digital economy.[137] In the specific context of source code, Mitchell et al., have noted that regulators 'can only require access to source code in exceptional cases where the general exceptions' in the GATS would be applicable,[138] underlining the inadequacy of such exceptions in light of evolving regulatory interests in the governance of code and algorithms, but also disregarding provision-level policy safeguards.

Indeed, provision-level carve-outs and exceptions are specific to the concrete subject matter at issue, and they show a high degree of experimentation in how parties to a treaty calibrate digital trade liberalization (concerning a specific policy issue) against the need to retain policy space. There are a few reasons to pay more attention to how carve-outs and exceptions have been integrated at the 'provision-level'. For one thing, not all treaties include applicable chapter-level general and security exceptions. The recently concluded US agreements with Taiwan, Malaysia, and Cambodia do not include any reference to general or security exceptions. Second, and more importantly, provision-level carve-outs and exceptions are not fully standardized, reflecting evolving (and more contemporary) approaches to what parties understand as crucial spaces to safeguard when it comes to software, and if applicable, algorithm governance. For this reason, Figure 2 presents the incidence of provision-level exceptions and carve-outs, which are specific to source code, for all those treaties that contain a binding provision on source code (currently 39).

[132] See generally J.E. Viñuales (2020) 'Seven Ways of Escaping a Rule: Of Exceptions and Their Avatars in International Law', in L. Bartels and F. Paddeu (eds), *Exceptions in International Law.* Oxford University Press, 67–70.

[133] See generally Burri and Kugler, supra n. 18.

[134] General Agreement on Trade in Services, 15 April 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869UNTS 183, 33 ILM 1167 (1994) ('GATS').

[135] General Agreement on Tariffs and Trade 15 April 1994, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 UNTS 187, 33 ILM 1153 (1994) ('GATT').

[136] See M. Vásquez Callo-Müller et al. (2027) 'The Breadth and Depth of Digital Trade Rulemaking: An Analysis Based on TAPED', in M. Burri and A. Chander (eds), *The Cambridge Handbook of Digital Trade Law*. Cambridge University Press.

[137] For a critique of those exceptions, particularly when applied to cybersecurity, see S. Peng (2023) 'Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions', *AJIL Unbound* 117, 122–127.

[138] A.D. Mitchell et al. (2023) 'AI Regulation and the Protection of Source Code', *International Journal of Law and Information Technology* 31, 4, 283.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

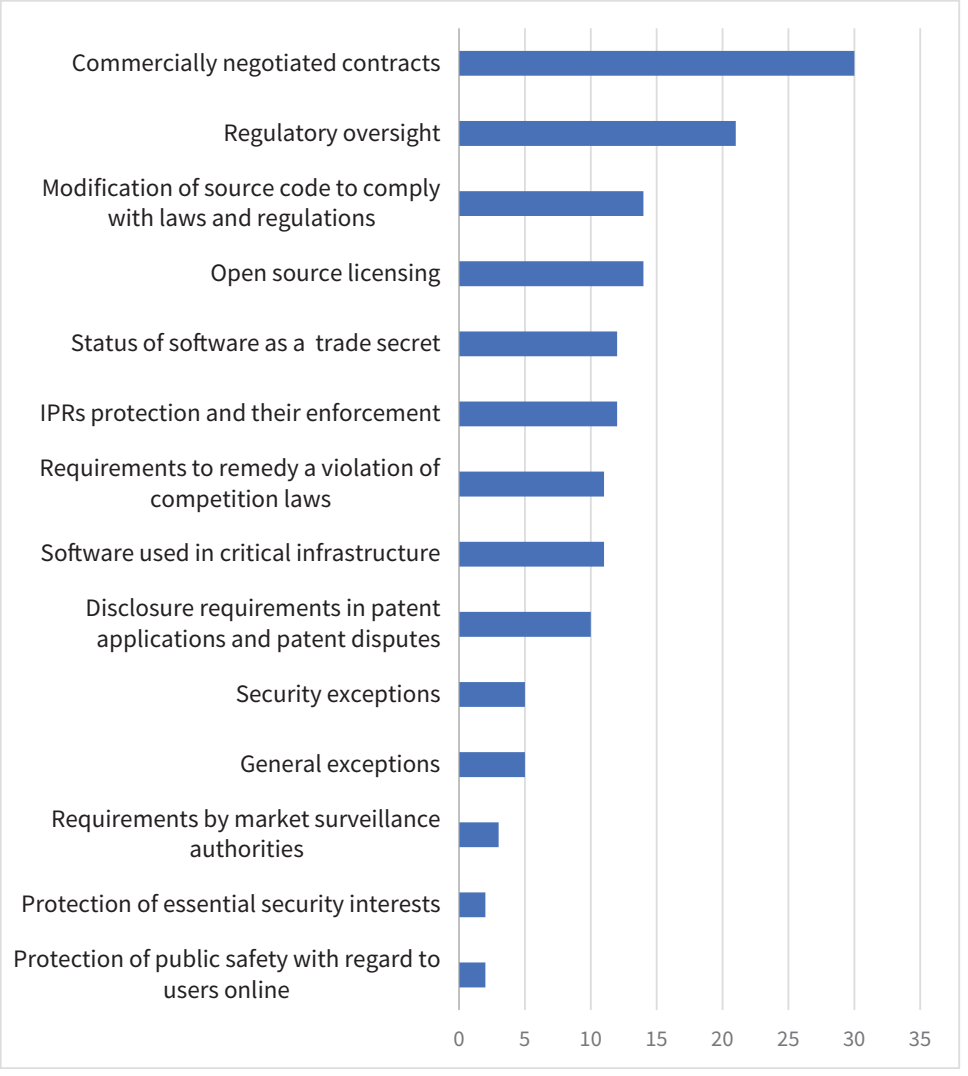


Figure 2. Frequency of carve-outs and exceptions in source code provisions (provision-level).
Source: Author's elaboration, based on TAPED, for 39 FTAs and DEAs under analysis.

4.2 Conceptual Distinction between Carve-Outs and Exceptions

Before proceeding further with the analysis of provision-level carve-outs and exceptions for source code (Figure 2), a theoretical approach is needed to distinguish exceptions from carve-outs. Carve-outs are defined categories of sectors or policy measures that are excluded from the scope of the agreement or the norm.[139] In treaty-making practice, carve-out clauses usually start with the language '[t]his Agreement [or chapter] does not apply to.'[140] Carve-outs effectively remove defined categories of government action from the treaty's scope or from certain obligations.[141] In the context of digital

[139] Ibid, 291.
[140] CPTPP, Article 14.2 (3).
[141] For an overview of the practice of carving-out sectors or measures from the scope of International Investment Treaties, see J. Paine and E. Sheargold (2023) 'A Climate Change Carve-Out for Investment Treaties', *Journal of International Economic Law* 26, 285, 292.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

trade, common exemptions (or carve-outs) include 'government procurement, information collected by or for the government, internal taxation, financial services, audio-visual services (or broadcasting), and gambling and betting services'.[142]

Carve-outs can be distinguished from exceptions such as those in Article XX of the GATT and Article XIV of the GATS, which act as affirmative defences.[143] The threshold to meet the requirements of Article XX of the GATT is quite rigorous.[144] A Party invoking the exception must prove a two-tier test. First, it must demonstrate that the measure falls within one of the specific exceptions listed in paragraphs (a) to (j) in Article XX of the GATT. This involves showing that the measure is 'necessary' to achieve the stated objective. Once a measure is provisionally justified under one of the paragraphs of Article XX of the GATT, the second tier of the test requires a WTO Member to demonstrate that the measure is 'not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade', according to the chapeau of GATT Article XX.[145] According to some scholars, the stringency of these legal tests poses the risk that certain regulatory measures, including in the digital realm, could be hard to justify.[146] Carve-outs, in contrast, exclude, at the outset, certain measures from the primary norm.[147] Therefore, the measures covered under the carve-out do not enter, *a priori*, into the regulatory gravitas of the primary norm, which, if carefully selected, provides for a wider scope for government regulatory activity. In addition, in some instances, carve-outs have been broadly interpreted. Following the examples provided by Viñuales, arbitration tribunals in international investment law tend to interpret the term 'procurement' broadly as a carve-out.[148]

That said, in some cases, and precisely because of the dynamic and evolving nature of how carve-outs and exceptions are incorporated within source code provisions, the policy safeguards (for lack of a better word) to protect regulatory space in this specific area evade a clear characterization as broader carve-outs or narrower exceptions. There are indeed cases where it seems evident that the Parties to a treaty intended to exclude specific measures from the scope of application. In those cases, there is little doubt of the characterization of those excluded measures as carve-outs. For example, the EFTA-Moldova FTA explicitly states that:

> 2. This Article *shall not apply to*:
>
> (a) requirements by a court or administrative tribunal;
> (b) intellectual property rights and their protection and enforcement;
> (c) competition law and its enforcement;
> (d) the right of a Party to take measures in accordance with Chapter 7 (Government Procurement);
> (e) requirements by market surveillance authorities in order to verify the conformity of goods and services with legal requirements; or
> (f) voluntary transfer or granting of access to source code on a commercial basis by a natural or juridical person of a Party. (emphasis added)

[142]Burri and Kugler, supra n. 18, 405.

[143]Viñuales, supra n. 134, 74.

[144]On the legal tests, see P.C. Mavroidis and M. Wu (2013) *The Law of the World Trade Organization (WTO): Documents, Cases and Analysis*, 2nd edn. West Academic Publishing, ch 12.

[145]Ibid.

[146]S. Peng (2024) *International Economic Law in the Era of Datafication.* Cambridge University Press, 32 (noting with regard to the Brazil-Taxation dispute that '[T]he mere fact that a responding party must have attempted to stretch the scope of the "public morals" exceptions to justify its digital inclusion policy within the WTO indicates that the interplay between international economic law and digital inequality invites further reflection').

[147]Viñuales, supra n. 134, 68.

[148]Ibid., 82.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

In other cases, however, it is difficult to distinguish between carve-outs and exceptions. Certain normative considerations support the view that, at least in some cases, the policy safeguards included in source code provisions – particularly, in the case of the non-EU FTAs and DEAs – constitute carve-outs, thus providing much more leeway and legal certainty to regulate software and AI algorithms. One might reasonably question, for example, whether regulators should subject the clarification that the source code provision applies only to mass-market software to an exception-based justification test. Both the policy rationale (the protection of a specific area) and the treaty language suggest that, in some cases, the parties intended such measures to delineate the boundaries of the obligation itself rather than to serve as ex-post justifications within its scope. The relevant provision in the CPTPP clearly exemplifies this, providing that it 'is limited to mass-market software or products containing such software and thus does not include software used for critical infrastructure'.[149] Mindful of the nuances described above, a systematic review of the policy safeguards included in source code provisions (Figure 2) reveals a limited set of consistent practices. These are listed in the next section to show their frequency – without classifying them as carve-outs or exceptions, which requires a case-by-case analysis.

4.3 Recurring Policy Safeguards in Source Code Provisions

In 30 out of 39 of the FTAs, parties include policy safeguards regarding *commercially negotiated contracts*, usually stating that: 'Nothing in this Article shall preclude: (a) the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts'.[150] This safeguard has been included across EU and non-EU agreements, including in the AfCFTA Digital Trade Protocol.[151] The evident implication of this safeguard is that private parties remain free to negotiate, in commercially negotiated contracts, the terms governing the provision of software, including access to or transfer of source code. An important aspect is that the safeguard may also extend to governments when they act as contracting parties in a commercial transaction, for example, in the context of public procurement. Article 12.11(3)(a) of the EU–New Zealand FTA specifically states that commercial basis shall be understood 'for example in the context of a public procurement transaction or a freely negotiated contract'. Such clarification provides sufficient leeway for states to require the disclosure or access to source code.

In about half of the cases (21 out of 39 FTAs), parties include a '*regulatory oversight safeguard*', whereby a regulatory body (or other entities, depending on the treaty language) can request the preservation and make available/transfer/or access the source code of software or, if applicable, algorithms, for specific investigation, inspection, examination, enforcement action, or judicial proceeding. Because of its relevance, this specific safeguard is analyzed in detail in sub-section 4.4.

Related to the above, 14 out of the 39 FTAs include a safeguard allowing a Party to require *modification of the source code of software necessary for that software to comply with laws or regulations which are not inconsistent with the relevant agreement*.[152] Initially incorporated in the CPTPP,[153] an outstanding aspect about this safeguard is the incorporation of the word 'necessary', which seems to indicate that this is, in fact, an exception, with a corresponding legal test. The scope of this safeguard is narrower than the regulatory oversight one, only allowing parties to request the modification of the source code or algorithm without explicitly requiring the transfer or access to it. Therefore, this safeguard provides regulators less leeway than the regulatory oversight safeguard.

In 14 out of 39 FTAs, parties to a treaty include a safeguard regarding *software licensing on a free and open-source basis*. This safeguard has different formulations. Sometimes, parties state that the source

[149] CPTPP, Article 14.17 (2).
[150] For example, Australia–Singapore DEA, Article 28 (3).
[151] See AfCFTA Digital Trade Protocol, Article 24 (3).
[152] For example, CPTPP, Article 14.17 (3) (b).
[153] CPTPP, Article 14.17 (3)(c).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

code provision 'does not apply to the voluntary transfer of, or granting of access to, source code of software by a person of the other Party, including an algorithm expressed in that source code …: (b) under open source licenses, such as in the context of open source coding'.[154] In other cases, a different formulation will be preferred: 'For greater certainty, nothing in paragraph 1 shall prevent a person of a Party from licensing its software on a free and open-source basis.'[155] This safeguard clarifies that private parties remain free to license software under free and open-source terms, including through licenses such as the Apache License. It does not, however, confer any right on a state to demand the provision of software or algorithms under an open-source license.

In less than a third of the cases (12 out of 39 FTAs), *specific safeguards regarding IP rights* will be included. Parties agree to the protection and enforcement of IP rights, stating that 'nothing in this Article shall affect: the protection and enforcement of intellectual property rights'.[156] In other cases, parties explicitly provide that the disclosure of source code 'shall not be constructed to negatively affect the software source code's status as a trade secret'.[157] Another clarification regarding IP found in 10 out of the 39 examined FTAs is that the source code provision 'shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to safeguards against unauthorized disclosure under the law or practice of a Party'.[158] EU treaties do not include this clarification since the general safeguard for IP protection and enforcement also covers disclosure requirements under patent law.

In less than a third of the cases (11 out of 39 FTAs), parties include a safeguard clarifying that *software used for critical infrastructure* falls outside the scope of the source code provision. In all those cases, there is no further explanation of what the parties understand as critical infrastructure. Typically, parties simply state that 'software … is limited to mass-market software or products containing such software and does not include software used for critical infrastructure'.[159] There is only one case in which this standard formulation varies, where the parties decide to include, not in the same category of critical infrastructure, but related to it, 'software that is specifically made for use by a Party'.[160]

Found primarily among EU treaties, and some EFTA agreements,[161] is the safeguard concerning *requirements by a court, administrative tribunal or competition authority to remedy a violation of competition law*.[162] This safeguard is included in 10 out of the 39 examined FTAs. Similarly, treaties that cover safeguards concerning *the protection of public safety concerning users online*, only include the EU–UK TCA[163] and the EU–India FTA.[164] Similarly, only found in EU treaties are an explicit reference to the applicability of *GATT and GATS exceptions* to the source code provision,[165] thus reiterating exceptions found at the chapter-level. Beyond EU treaties, only the Australia–Indonesia CEPA refers to *security exceptions*, noting that the relevant source code provision 'shall (not) prevent a Party from

[154]UK–Singapore DEA, Article 8.61-k (2) (2).

[155]For example, Australia–UK FTA, Article 14.8 (5).

[156]For example, EU–Singapore DTA, Article 11.

[157]Australia–Singapore DEA, Article 28, footnote 14.

[158]Australia–Indonesia CEPA, Article 13.13 (4) .

[159]Singapore–New Zealand CEPA, Article 9.13 (2).

[160]Australia–Indonesia CEPA, Article 13.13 (2). ('For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure, or software that is specifically made for use by a Party.')

[161]EFTA–Ukraine FTA, Article 4.14 (c); EFTA–Moldova FTA, Article 5.14 (c).

[162]For example, EU–Japan EPA, Article 8.73 (2)(b).

[163]EU–UK TCA, Article 207 (3)(b).

[164]EU–India FTA, Article X.11(3)(b).

[165]The agreed text for the EU–Korea DTA provides that:

'2. For greater certainty:

a) Article 28 [General exceptions], Article 29 [Security exceptions] and Article 27 [Prudential carve-out] may apply to measures of a Party adopted or maintained in the context of a certification procedure'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use , available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

adopting or maintaining any measures that it considers necessary for the protection of its essential security interests',[166] without specifically referring to Article XXI (b) of the GATT, nor the situations in which this exception may be invoked.[167]

It is important to clarify that the above policy safeguards do not include mandating the transfer of source code for technology transfer, promoting indigenous innovation or even digital sovereignty, which policy makers might envisage as a policy goal. For example, some governments could seek to include requirements in their government procurement contracts to make the source code of software available as open source. This can be seen as a policy to reduce reliance on proprietary solutions and achieve digital sovereignty. In November 2025, this was one of the points made by German Chancellor Friedrich Merz, noting that the use of open-source solutions in the public administration, such as openDesk, is a way to achieve digital sovereignty.[168] This aspect has not been raised explicitly in FTAs and DEAs. However, government procurement is generally carved out of the scope of digital trade chapters.[169] In some cases, government procurement will also be specifically included as a carve-out under the provisions on source code.[170] Along the same line, certain sectoral carve-outs applicable to the whole digital trade chapter include audiovisual and financial services.[171] When those carve-outs are included, at the chapter or provision level, measures that would affect the disclosure of source code provisions, for instance, in the financial services sector, are excluded from the scope of the agreement.

Beyond what is excluded, an aspect that stands out is what is included in some FTAs and DEAs, specifically in the case of EU FTAs. In the EU–New Zealand FTA, the parties added a preamble to the source code provision that recognizes the 'increasing social and economic importance of the use of digital technologies and the importance of the safe and responsible development and use of such technologies, including in respect of source code of software to foster public trust'.[172] This preamble is a soft and non-enforceable obligation, but it was incorporated to counter the fears that source code provisions will deprive states of their regulatory power over digital technologies. However, across the set of the 39 examined FTAs and DEAs, this is the only agreement that includes such language.

There has been a recurring tendency in the digital trade literature to understand many of the policy safeguards described earlier as exceptions, which inevitably subjects them to a higher threshold and reduces the regulatory space for governments.[173] However, this qualification to classify them as exceptions or carve-outs requires a case-by-case interpretation of the provision at issue.

4.4 The Regulatory Oversight Safeguard

One notable recurring safeguard in many agreements is the 'regulatory oversight' safeguard. First incorporated in the USMCA,[174] the regulatory oversight safeguard has subsequently been incorporated in more than half (namely, 21) of the FTAs and DEAs with source code provisions, but it has

[166] See Australia–Indonesia CEPA, Article 13.13.

[167] Article XXI (b) GATT provides 'Nothing in this Agreement shall be construed … (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests (i) relating to fissionable materials or the materials from which they are derived; (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment; (iii) taken in time of war or other emergency in international relations; or …'.

[168] Die Bundesregierung (2025) 'Summit on European Digital Sovereignty Delivers Landmark Commitments for a more competitive and sovereign Europe', www.bundesregierung.de/breg-de/aktuelles/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe-2394368 (accessed 11 April 2025).

[169] Burri and Kugler, supra n. 18.

[170] EU–Chile Advance Framework Agreement, Article 19.12 (2) (b).

[171] For example, in the case of financial services, see Chile–Paraguay FTA, Article 7.2. In the case of audiovisual services, see Australia–UK FTA, Article 14.2.

[172] EU–New Zealand FTA, Article 12.11 (1).

[173] Dorobantu et al., supra n. 25, 124–128; Słok-Wódkowska and Mazur (n. 10) 99–100; Irion, supra n. 10, 1564–1565.

[174] USMCA, Article 19.16 (2).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

not been incorporated in landmark agreements such as the CPTPP. It is furthermore the only safeguard included in the recent US agreements with Cambodia[175] and Taiwan.[176] By its legal design (a derogation from the binding obligation not to disclose source code), this safeguard can be classified as an exception. Because of this, the Party invoking this exception (that is, the state) bears the burden of proof. At its core, it concerns the right of a 'regulatory body' to require the preservation and making available,[177] transferring,[178] or accessing[179] the source code (and sometimes algorithms) for specific investigative or enforcement purposes, subject to safeguards against unauthorized disclosure. At the outset, FTAs and DEAs differ in determining what a 'regulatory body' is. In some cases, it can cover administrative bodies and judicial authorities.[180] In other cases, it can clarify that 'regulatory body' covers government agencies, law enforcement agencies, a regulatory body, or judicial authority.[181] Under FTAs and DTAs where the EU and the UK[182] are parties, a 'regulatory body' also covers conformity assessment bodies.[183]

Typically, the regulatory oversight safeguard begins with '[T]his article does not preclude' or, in the case of EU FTAs and DEAs, '[N]othing in this article shall affect the right of regulatory authorities to.'[184] What follows is the enunciation that a 'regulatory body' can request the preservation and make available/transfer/or access[185] to the source code of software or, if applicable, algorithms, for '*specific investigation, inspection, examination, enforcement action, or judicial proceeding*' (emphasis added). In some cases, the pertinent provision further clarifies that such an investigation, inspection, examination, enforcement action, or judicial proceeding is to secure compliance with laws and regulations, and to pursue legitimate public policy exceptions. This is particularly the case of the EU DTAs with Singapore and Korea.[186] A slightly broader formulation is also adopted in the AfCFTA Digital Trade Protocol.[187] Article 3 of the AfCFTA Annex on Source Code states the legitimate public policy reasons under which a state can justify its actions, which, by the use of the words 'such as', are illustrative. They resemble some aspects of the general exceptions included in GATT Article XX and GATS Article XIV, providing that:

> Article 3. Legitimate and Legal Public Interests
>
> In accordance with Article 24(2) of the Protocol, a regulatory body or judicial authority of a State Party may require a person of another State Party to preserve and make available the source code of the software or an algorithm expressed in that source code, subject to safeguards against unauthorised disclosure under the law or practice of a State Party, in order to pursue legitimate and legal public interest objectives *such as* to:
>
> a) maintain public order and safety;
> b) protect public morals;
> c) protect human, animal or plant life or health;

[175] See supra n. 34.
[176] See supra n. 35.
[177] USMCA, Article 19.16 (2).
[178] UK–Japan CEPA, Article 8.73 (2)(b).
[179] EU–New Zealand FTA, Article 12.1(4)(a).
[180] USMCA, Article 19.16 (2).
[181] Korea–Singapore Digital Partnership Agreement, Article 14.19(2).
[182] For example, UK–Singapore DEA, Article 8.61-K(3); Australia–UK FTA, Article 14.18 (2).
[183] Article 11 of the corresponding EU–Singapore and Korea DTAs.
[184] EU–New Zealand FTA, Article 12.1(4)(a).
[185] Ibid.
[186] Article 11(3) of the corresponding EU–Singapore and EU–Korea DTAs.
[187] AfCFTA Digital Trade Protocol, Article 24(2). (This Article does not preclude a regulatory body or judicial authority of a State Party from requiring a person of another state Party to preserve and make available the source code of software or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, audit, enforcement action, or judicial proceeding *or when required* for legitimate and legal public interest reasons) (emphasis added).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

d) protect essential security interests;
e) access to critical infrastructure;
f) prevent deceptive and fraudulent practices; or
g) prevent arbitrary or unjustifiable discrimination.

It is important to note that the legitimate public policy reasons outlined in Article 3 of the AfCFTA Annex on Source code are not further explained in subsequent sections of the same Annex, leaving key terms such as 'critical infrastructure' or 'essential security interests' undefined. However, in contrast to other FTAs and DEAs, which contain much more succinct language, Article 4 of the AfCFTA Annex on Source code establishes a set of conditions for applying this exception, providing that:

> A regulatory body or judicial authority of a State Party … shall not apply Article 3 of this Annex in a manner in which: a) constitutes a disguised restriction to digital trade or dishonest commercial practice; b) constitutes means of arbitrary or unjustifiable discrimination; c) unreasonably prejudices the legitimate interests of the affected person of a State Party; d) is inconsistent with the protection and enforcement of intellectual property rights in the AfCFTA digital market; or e) restricts digital trade more than necessary to achieve legitimate and legal public interest objectives.

In the case of the EU DTAs, the elucidation of what is a legitimate public policy objective is achieved through a cross-reference, via a footnote, to the legitimate public policy objectives included in the cross-border data flows provision.[188] These encompass online safety, cybersecurity, safe and trustworthy AI, protection against the dissemination of disinformation, and or other comparable objectives. Interestingly, the interpretation of the legitimate public policy objectives shall be determined by taking into account the 'evolving nature of digital technologies and related challenges',[189] possibly allowing for an evolutionary interpretation of the legitimate public policy objectives. This approach is unique to the EU model, differentiating it from other FTAs and DEAs, and seems designed to shield, by all possible means, the ability of EU regulators to require the disclosure or the transfer of source code.

A further innovation found in recent UK FTAs, such as the India–UK FTA, is the inclusion of a footnote clarifying that this regulatory oversight exception applies 'to a requirement to preserve and make available the source code of software that is designed to promote algorithmic accountability in furtherance of or following an investigation, inspection, examination, enforcement action, or judicial proceeding',[190] thereby placating previous scholarly critics on the incorporation of source code provisions in UK FTAs and DEAs,[191] and clarifying the ability of regulators to effectively regulate algorithms.

It should be noted that beyond the case of the AfCFTA and EU FTAs and DTAs, the regulatory oversight exception only has a thin association with the corresponding exceptions in the GATT and GATS frameworks, as if parties to the relevant treaties were intentionally departing from them and their controversial application and, thus setting a new path for preserving regulatory space. For instance, in none of the cases is it mentioned that access to source code or algorithms, under the

[188] See EU–Korea DTA, Article 11 (3) (a), footnote 13. (These may include those listed in footnote 5 [list of legitimate public policy objectives] to Article 5.3 [Cross-border data flows]).

[189] EU–Korea DTA, Article 5, footnote 5. ('For the purpose of this Article, "legitimate public policy objective" shall be interpreted in an objective manner and shall enable the pursuit of objectives such as the protection of public security, public morals, or human, animal or plant life or health, the maintenance of public order, the protection of other fundamental interests of society such as online safety, cybersecurity, safe and trustworthy artificial intelligence, or protecting against the dissemination of disinformation, or other similar objectives of public interest, taking into account the evolving nature of digital technologies.'). See also EU–Singapore DTA, Article 5, footnote 1.

[190] India–UK CETA, Article 12.15 (2)(a), footnote 11.

[191] Jones, supra n. 10.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

regulatory oversight exception, shall be 'necessary', or that the measure at issue shall not be 'applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination … or a disguised restriction on international trade'.[192] None of the source code provisions reproduces, or closely resembles, the wording of the chapeau to GATT Article XX. Therefore, it may not be necessary for states to pass a stringent legal test to invoke the regulatory oversight exception. The US–Japan DTA illustrate this clearly:

> 2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of the other Party to preserve and make available the source code of software, or an algorithm expressed in that source code, for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure.[193]

4.5 Implications

The overview of the frequency of safeguards applicable to the non-disclosure of source code at the provision-level in FTAs and DEAs shows that the balance between protection and disclosure is not solely mediated through horizontal trade exceptions (chapter-level exceptions), as sometimes assumed in the scholarly literature. Instead, it is also determined by an evolving (and quite technical) array of provision-level carve-outs and exceptions, which, given the diverse formulation in treaty practice, have been untangled here only as 'policy safeguards'. The variety of currently covered circumstances under these safeguards showcases the most pressing aspects, which, in the view of trade negotiators, lie at the intersection of digital trade liberalization and code and algorithm regulation and governance. While there is significant variation across agreements, there is certain elucidation on the fundamental public interests at stake, particularly under the latest EU and UK agreements, which are the regions with corresponding advanced domestic legal frameworks regarding AI governance. In this sense, while some models are emerging (for instance, the highly elaborated EU model, or the 'minimalistic' US model), these themselves continue to evolve, showcasing ongoing contestation of how to better protect source code and algorithms under digital trade law, while at the same time allowing the preservation of policy space.

5. Conclusions

The current international IP regime falls short of adequately safeguarding the interests of software and AI developers in protecting source code and algorithms when these enter the government sphere. As a result, and compounding fears of forced technology transfer, the protection of software's source code and, when applicable, algorithms have migrated to an adjacent field: digital trade law. Source code provisions in digital trade rulemaking provide an ex-ante layer of protection for source code – and, in some cases, algorithms – irrespective of their eligibility for protection under IP law. In addition, when software and algorithms may find protection under different IP rights, source code provisions in digital trade law act as an additional layer of protection.

As the function of source code provisions is to establish a ban against disclosure or transfer of software source code and, in some cases, algorithms, this domain shift carries systemic consequences for the mechanisms to achieve a balance between protection and disclosure. In the IP realm, striking such a balance will typically be determined, on a case-by-case basis, by the internal IP limiting mechanisms, such as thresholds for protected subject matter. However, balancing mechanisms in digital trade law differ in nature from those in IP law and rely instead on applicable carve-outs (such as for

[192] See Chapeau to Article XX GATT (General exceptions).

[193] US–Japan DTA, Article 17. Compare with Malaysia–US Reciprocal Trade Agreement, Article 3.4(2)(e); Cambodia – US Reciprocal Trade Agreement, Article 3.4; US–Taiwan Trade Agreement, Article 4.4.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578

government procurement or exclusion of certain sectors, such as the audiovisual or financial sector) and exceptions. These can apply horizontally to the entirety of digital trade chapters, but increasingly, these can be included at the provision-level, mediating in a more contemporary and technical way the balance between protection and disclosure as it relates to a specific subject matter. These provision-level mechanisms are particularly attractive as a matter of treaty design, as they can more clearly reflect regulatory priorities in fast-moving digital markets. However, their formulation varies significantly across agreements: revealing limited agreement on which public interests should be protected; the different stages of AI domestic regulatory developments and their reflection into international treaty-making; and how to incorporate regulatory priorities into the strategic design of treaties.

Among the most relevant policy safeguards outlined in the Article, the regulatory oversight exception, included in more than half the agreements examined here, but absent in landmark agreements such as the CPTPP, is the most relevant for AI transparency measures aimed at ensuring the safety and trustworthiness of algorithmic systems. Overall, despite the differences across agreements, the tailoring of these different provision-level policy safeguards indicates more space for future experimentation according to specific circumstances, and provides an overview of the different mechanisms that governments should be compelled to employ to ensure future code and algorithm regulation and governance.

Acknowledgements. An initial version of this paper was presented at the 19th Annual Conference of the European Policy for Intellectual Property Association (EPIP) in Pisa, Italy (September 2024), at a workshop at the Centre for Global Law and Innovation at the University of Bristol (March 2025), and at the SIEL Conference 2025 in Taipei. The author would like to thank the participants in all three events for their thoughtful comments on earlier versions of this paper, as well as the anonymous reviewers for their insightful revisions, which substantially improved the paper.

Cite this article: M. Vásquez Callo-Müller (2026) 'Regulating Source Code in Trade Agreements: Between Protection and Disclosure', *World Trade Review* 25(4), 556–582. https://doi.org/10.1017/S1474745626101578

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 21:50:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1474745626101578