United Nations A/CN.9/1117

General Assembly

Distr.: General
27 April 2022

Original: English

United Nations Commission on International Trade Law
Fifty-fifth session
New York, 27 June–15 July 2022

Legal issues related to digital economy – proposal for future work on data transactions

Note by the Secretariat

Contents

V.22-02480 (E) 050522 060522

I. About this note

1. This note presents a proposal for future work by Working Group IV on data transactions which builds on discussions on the topic at the Commission during its fifty-fourth session. It is the product of preparatory work that the secretariat has carried out on the topic, as requested by the Commission at that session,[1] as well as preliminary discussions on the nature and scope of possible future work that took place at the most recent session of Working Group IV[2] in line with the suggestion that the topic might eventually be referred to the Working Group to be dealt with in tandem with the topic of automated contracting.[3] Future work by the Working Group on the topic of automated contracting is the subject of the proposal contained in chapter II of A/CN.9/1116.

2. After recalling the background to exploratory and preparatory work on the topic of data transactions (chap. II), this note defines key concepts related to the topic (chap. III), outlines the legal issues to be addressed with respect to the two aspects of the topic, namely data contracts (chap. IV) and data rights (chap. V), and puts forward a proposal as to how Working Group IV could be mandated to proceed in addressing those legal issues (chap. V).

II. Background

A. Consideration of the topic within the Commission

3. The exploratory and preparatory work by the secretariat on data transactions stems from a mandate given by the Commission at its fifty-first session (2018) for the secretariat to "compile information on legal issues related to the digital economy".[4]

4. At its fifty-second session (2019), the Commission heard that the secretariat's exploratory work on legal issues related to the digital economy had identified several lines of enquiry that might crystallize into more concrete proposals to be submitted to the Commission for consideration.[5] One such line of enquiry was the rights of parties to data transactions for commercial purposes. The Commission requested the secretariat to continue its exploratory work and to prepare a workplan to address the specific legal issues identified in the course of that exploratory work.[6]

5. For its fifty-third session (2020), the Commission received a progress report from the secretariat on its exploratory work (A/CN.9/1012) which put forward a workplan for addressing specific legal issues identified in the course of that work. Among other things, the workplan identified two aspects of the topic of data transactions – (i) the rights and obligations of parties to data transactions, and (ii) rights in data as a commodity. The workplan suggested that preparatory work proceed on the first aspect, while further exploratory work be carried out on the second aspect. Broad support was expressed in the Commission for work to continue in accordance with the workplan.[7] It was also noted that the various topics addressed in the workplan were interconnected and interdependent, particularly artificial intelligence and data transactions, and therefore that work on one topic may raise the need to address other topics.[8]

---

[1] *Official Records of the General Assembly, Seventy-sixth Session, Supplement No. 17* (A/76/17), para. 237.
[2] As noted in para. 7 below, those are reported in chapter VI of A/CN.9/1093.
[3] *Official Records of the General Assembly, Seventy-sixth Session, Supplement No. 17* (A/76/17), para. 237.
[4] Ibid., *Seventy-third Session, Supplement No. 17* (A/73/17), para. 253(b).
[5] Ibid., *Seventy-fourth Session, Supplement No. 17* (A/74/17), para. 209.
[6] Ibid., para. 211.
[7] Ibid., *Seventy-fifth Session, Supplement No. 17* (A/75/17), part two, para. 70.
[8] Ibid., para. 75.

6. For its fifty-fourth session (2021), the Commission received a progress report from the secretariat which provided an update on preparatory work on the rights and obligations of parties to data transactions (A/CN.9/1064, paras. 15-23). Broad support was expressed in the Commission for the secretariat to continue preparatory work on data transactions, and it was suggested that the topic might eventually be referred to Working Group IV to be dealt with in tandem with the topic of the use of artificial intelligence and automation in contracting.[9]

B. Consideration of the topic within Working Group IV

7. At its sixty-third session (4-8 April 2022), Working Group IV agreed to set aside time for a preliminary discussion of the nature and scope of possible future work on data transactions. The Working Group engaged in an exchange of views on the legal issues to be addressed in a possible harmonized legal framework for data transactions, as well as on a range of conceptual and scope issues that could frame future work on the topic. The deliberations of the Working Group on those issues, which are reported in chapter VI of A/CN.9/1093, have been incorporated into this note.

III. Concepts and scope

A. "Data"

8. Through its work developing a legal taxonomy of emerging technologies and their applications (as reported in chapter III of A/CN.9/1116), the secretariat has developed a working definition of "data" as a representation of information in electronic form. The working definition is based on the widely-used definition of "data", formulated by the International Organization for Standardization (ISO), as "a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing".[10] A similar understanding of data – as a representation of information – underlies the notion of "data message" in UNCITRAL texts on e-commerce, which is defined as "information generated, sent, received or stored by electronic, magnetic, optical or similar means" (i.e. other than by paper-based means).[11] More recently, the recommendation by the Council of the Organisation for Economic Co-operation and Development (OECD) on enhancing access to and sharing of data[12] defines data, in somewhat less technical terms, as "recorded information in structured or unstructured formats".

9. On the basis of the ISO definition, data need not be in electronic form or in a machine-readable format.[13] Nevertheless, it is the quality of machine-readability – and thus suitability for automated processing – that gives data greater potential value in the digital economy, facilitating the production of "digital intelligence" to inform decision-making and the development of new products. For that reason, the 2021 Principles for a Data Economy, jointly developed by the American Law Institute (ALI) and the European Law Institute (ELI) ("ALI/ELI Principles"),[14] define "data" to mean "information recorded in any machine-readable format suitable for automated processing, stored in any medium or as it is being transmitted".[15]

---

[9] Ibid., *Seventy-sixth Session, Supplement No. 17* (A/76/17), para. 237.

[10] ISO, *Information Technology – Vocabulary*, ISO/IEC Standard No. 2382, 2015.

[11] See, e.g., UNCITRAL Model Law on Electronic Commerce, art. 2(a); United Nations Convention on the Use of Electronic Communications in International Contracts (2005), art. 4(c).

[12] OECD, Recommendation of the Council on Enhancing Access to and Sharing of Data (2021), document C/MIN(2021)20/FINAL.

[13] A note to the definition of "data" in ISO/IEC Standard No. 2382 states that data "can be processed by humans or by automated means".

[14] In this note, reference is made to the version of the ALI/ELI Principles contained in "ELI Final Council Draft", which is available at www.principlesforadataeconomy.org/ (accessed on 27 April 2022).

[15] ALI/ELI Principles, principle 3(1)(a).

10. The working definition of "data" covers a wide variety of information that has become the subject of commercial transactions, including market analysis data and operational data (e.g., data generated by sensors attached to machines). As the secretariat has identified in its exploratory work (see A/CN.9/1012/Add.2), data has become a global commodity that generates value and drives innovation. The importance of data was emphasized by the Secretary-General in the preface to the most recent Digital Economy Report by the United Nations Conference on Trade and Development (UNCTAD), in which he stated:

> "Data have become a key strategic asset for the creation of both private and social value. How these data are handled will greatly affect our ability to achieve the Sustainable Development Goals. Determining what is the best way forward will be difficult but necessary. Data are multidimensional, and their use has implications not just for trade and economic development but also for human rights, peace and security."[16]

11. The key to generating value from data lies in its "processing", which refers to the various operations that can be performed on data, including collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, transmitting, aligning or combining, and restricting, erasing or destroying. In less technical terms, one or more of those operations may be involved in "accessing", "sharing", "using" and "disclosing" data, which are concepts that are more often referred to in existing law and contractual provisions relating to data. Similarly, performing one or more of those operations on data may evidence the "holding" or "control" of that data, and may result in the "generation" of new data (i.e. "derived data").

12. Data is sometimes categorized into different types, including by reference to (i) the person who controls the data (e.g. public data, private data), (ii) the person to whom the data relates (e.g. personal data, customer data), (iii) the content or purpose of the data (e.g. proprietary data,[17] corporate data, technical data), and (iv) the format of the data (e.g. structured data, unstructured data). Those categories, which often overlap, indicate that data and data transactions engage a wide range of actors and a wide range of laws (as elaborated in the section on "data transactions" below).

13. At the sixty-third session of Working Group IV, it was observed that the working definition developed by the secretariat was quite broad and that transactions in "data", so defined, could extend to dealings in digital assets. After all, digital assets – understood as an electronic record capable of being controlled and uniquely identified, including an "electronic transferable record" within the meaning of the UNCITRAL Model Law on Electronic Transferable Records – are constituted or represented by data.[18] By a similar token, transactions in "data" could also extend to transactions for the transfer or supply of software (i.e. computer code in the form of data). Arguably, dealings in digital assets and software transactions are not concerned with data as a representation of "information" – in the sense of material that can be given meaning in a particular context – but rather with data as the means to effect processes that give software and digital assets their value. For that reason, the ALI/ELI Principles expressly exclude "functional data" (i.e. "data the main purpose of which is to deliver particular functionalities") and "representative data" (i.e. "data the main purpose of which is to represent other assets or value") from scope.[19] In the case of digital assets, the UK Jurisdiction Taskforce (a taskforce of the LawTech Delivery Panel established by the Government of the United Kingdom of Great Britain and Northern Ireland, the judiciary of England and Wales, and the Law Society of England and Wales) has explained that "it is not what the data [representing a

[16] UNCTAD, *Digital Economy Report 2021 – Cross-border Data Flows and Development: For Whom the Data Flow* (Geneva, 2021), p. iv.

[17] The notion of "proprietary data" is understood as data that is subject to "data rights" as described in para. 27 below, in particular protections afforded under laws relating to trade secrets, copyright or database rights.

[18] This working definition of digital assets is developed in A/CN.9/1012/Add.3, para. 7.

[19] ALI/ELI Principles, principle 2(1).

digital asset] tells you but what it allows you to do".[20] Similar explanations have been offered in commentary to distinguish software.

14. In view of existing legal regimes for software transactions and electronic transferable records, as well as the need to coordinate with ongoing work at Unidroit on digital assets and private law (see A/CN.9/1107), it is proposed that future work on data transactions focus on data other than data constituting or representing digital assets or data in the form of computer code. At the sixty-third session of Working Group IV, it was suggested that the approach taken in the ALI/ELI Principles could be considered as a starting point for distinguishing those other transactions.

B. "Data transactions"

15. "Data transactions" are transactions that are concerned with data; specifically, the control or processing of data.[21] Ordinarily, data transactions occur under contract (i.e. "data contracts").

16. At the sixty-third session of Working Group IV, a question was raised as to whether data rights could properly be characterized as an aspect of data transactions, particularly insofar as those rights exist outside a contractual relationship. As noted above (para. 5), the secretariat has examined the rights and obligations of parties to data transactions, as well as rights in data as a commodity (i.e. "data rights"), under the overarching topic of "data transactions". Although data rights often arise from data transactions (e.g. they can be created by a transaction involving the relevant rightholder, as in the case of "co-generated data" discussed in para. 53 below) and are engaged by data transactions (e.g. they can be violated by a transaction involving the relevant data), the types of data rights contemplated for future work (as elaborated in the section on "data rights" below) are independent of contract. While retaining the reference to "data transactions" as the topic for future work, this note refers simply to "data contracts" and "data rights" to describe the two aspects of the topic.

17. Data transactions also occur along a "data value chain" which involves multiple actors. Those actors may be defined by the roles that they perform along the data value chain at a given point in time, which often overlap, including: (i) data generator (the person who generates data, including by way of a machine or sensor), (ii) data subject (the person to whom data relates, whether a legal person or natural person), (iii) data provider (the person who provides data, who may also be a data generator, data subject or data controller), (iv) data recipient (the person who receives data, who may also become a data processor or data controller under a data transaction), (v) data controller (the person who "holds" data or "controls" how the data is processed), and (vi) data processor (the person who processes data, which encompasses almost all other roles but often refers to persons in contradistinction to the data controller).

18. The various actors and operations performed on data, together with the data transactions between then, comprise the "data ecosystem".[22] At the sixty-third session of Working Group IV, it was stressed that future work on data transactions should take into account the complexities of the data ecosystem. In particular, it was observed

[20] "Legal Statement on Cryptoassets and Smart Contracts", November 2019, para. 30, available at https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf, para. 60.

[21] Admittedly, all electronic transactions involve some exchange of data (e.g. the electronic identification of the parties, application of electronic signatures by the parties, and the exchange of electronic communications forming an electronic contract), but that data is not the subject of those transactions.

[22] The recommendation by the Council of the OECD on enhancing access to and sharing of data, see footnote 8 above, defines the "data ecosystem" as "the integration of and interaction between different relevant stakeholders including data holders, data producers, data intermediaries and data subjects, that are involved in, or affected by, related data access and sharing arrangements, according to their different roles, responsibilities and rights, technologies, and business models".

that future work should clearly define what it means to "hold" or "control" data, which may be particularly relevant in the context of data rights.

19. Data transactions engage a variety of different legal regimes, each of which imposes a "layer" of rights and obligations among the parties to data transactions as well as other third party actors along the data value chain. If the data contract forms the "base" layer for the rights and obligations of the parties, privacy and data protection laws, as well as laws relating to trade secrets, copyright and database rights, provide additional layers depending on the type of data being transacted. The Commission has indicated that future work should avoid privacy and data protection issues, as well as intellectual property issues.[23] At its sixty-third session, the Working Group IV considered what it meant for future work to avoid privacy (specifically, data privacy) and data protection issues. In summary, the following views were exchanged:

(a) Avoiding data privacy and protection issues means that future work should not only be aware of relevant laws, but also refrain from harmonizing regulatory measures concerning the processing of personal data. It also means that a baseline for future work should be a requirement that data be processed "lawfully";

(b) Avoiding data privacy and protection issues does not mean that future work should ignore data that, in a particular jurisdiction, is regarded as "personal data". It would be impractical – if not impossible – to limit the scope of future work to data other than personal data. In that regard, it is worth noting that the principles and policy guidance set out in the recommendation by the Council of the OECD on enhancing access to and sharing of data (see para. 8 above) apply to all types of data, including personal data.

20. The Commission has also indicated that future work should avoid overlap with work being carried out within the United Nations system and other international forums.[24] One point of perceived overlap concerns personal data. If data being transacted is "personal data", one way to avoid overlap with the work being done in international forums, including the Council of Europe in the context of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,[25] as amended, is for future work to preserve all applicable regulatory measures concerning the processing of personal data.

21. Another point of perceived overlap concerns data governance and cross-border data flows, which are becoming a focus of international trade and cooperation for all types of data, including within the United Nations system.[26] If anything, future work has the potential to complement – rather than duplicate – those initiatives, much as UNCITRAL work has done in other areas, including with respect to the work of the World Trade Organization in the areas of e-commerce and public procurement:

(a) One example is provided by ongoing efforts among members of the World Trade Organization to negotiate rules to enable and promote the flow of data as part of the Joint Statement Initiative (JSI) on E-Commerce. The drafting proposals for such rules that have been published so far are focused on overcoming regulatory barriers, such as localization requirements for data processing or other restrictions on the cross-border transfer or data, and on declaring broad policy objectives to establish a permissive regime for data flows that facilitate international trade. The proposals do not address how those flows are effected, whether internally (e.g. data transfer within an organization) or between different actors in the data value chain (e.g. data transfer under a data contract). Accordingly, they do not address the private law gaps that inhibit data transactions, as outlined below (see para. 29 on data contracts and para. 46 on data rights), nor do they mandate harmonized responses to pre-empt

[23] *Official Records of the General Assembly, Seventy-fifth Session, Supplement No. 17* (A/75/17), part two, para. 75.

[24] Ibid., para. 72.

[25] United Nations, *Treaty Series*, vol. 1496, No. 25702.

[26] UNCTAD, *Digital Economy Report 2021 – Cross-border Data Flows and Development: For Whom the Data Flow* (Geneva, 2021), p. xx.

fragmented national legislative efforts to fill those gaps, which could create further obstacles to international trade. Future work on data transactions could thus provide the basic legal infrastructure to give effect those policy objectives, much as existing UNCITRAL texts on e-commerce do for rules enabling e-commerce that are also being negotiated as part of the JSI, and which already exist in bilateral and regional free trade agreements (including dedicated digital trade agreements);

(b) Another example is provided by the recommendation by the Council of the OECD on enhancing access to and sharing of data (see para. 8 above). The recommendation recognizes that data access and sharing arrangements encompass not only the institutional, regulatory and policy frameworks that determine the conditions of data access and sharing, but also the legal and contractual frameworks. Insofar as the recommendation does not prescribe standards for contractual frameworks (although it does recognize the importance of party autonomy), future work on data contracts could provide an important contribution to the development of such standards.

C. "Data contracts"

22. As noted above (para. 15), "data contracts" are contracts for the control or processing of data for commercial purposes. Data contracts can be categorized by reference to the role played by each party. In that regard, a rough distinction can be drawn between "data provision" and "data processing" contracts. Broad support was expressed at the sixty-third session of Working Group IV for applying the distinction as a basis for future work.

1. Data provision contracts

23. A data provision contract essentially involves a person (the "data provider") providing data to another person (the "data recipient") for the other person to use or otherwise process. In broad terms, data provision may be likened to the "sale" or "licensing" of data, depending on the control that the data provider retains over the data. For example, at the sixty-third session of Working Group IV, it was noted that contracts for the provision of data that is accessible only on a system controlled by the data provider might apply a "licence approach", while contracts for the provision of data that can be accessed and used by the data recipient outside such a system might apply a "sales approach". Data can be provided by "sharing" the data or by giving the data recipient "access" to the data. "Sharing" and "accessing" are therefore opposite sides of the same data transaction.

2. Data processing contracts

24. A data processing contract involves a person (the "service provider") processing data for another person (the "service recipient") and providing the processed data to the other person. Common types of data processing transactions include data scraping, cloud-based services, data analytics, and electronic transmission services. While data processing contracts involve the provision of data between the parties (e.g. data provided by the service recipient to be processed and the resulting processed data provided by the service provider), they are predominantly concerned with the provision of services.

3. Other types of data contracts?

25. As noted above (para. 22), the separate treatment of data provision and data processing contracts involves a rough distinction, which is demonstrated by the use of online platforms. As the secretariat has observed in its exploratory work on data transactions [27] and online platforms, [28] online platforms support not only data

[27] See A/CN.9/1012/Add.2, para. 12.
[28] See A/CN.9/1064/Add.3, para. 5.

processing (by the platform operator) but also data provision (between platform users). Some online platforms establish a "data marketplace" or are operated by "data intermediaries". At the sixty-third session of Working Group IV, a query was raised as to how data marketplace contracts and contracts with data intermediaries fit within the categories of data contracts described above (para. 22). Consistent with the contractual structure of online platforms that has previously been described by the secretariat,[29] it is suggested that the contract between the operator of the data platform and the platform user would ordinarily be a data processing contract, while the contract between platform users would ordinarily be a data provision contract. As outlined below (chap. IV), each of these contracts and the relationships that they establish entail different business needs and raise different legal issues.

D. "Data rights"

26. The notion of "data rights" (or "rights in data") is not yet firmly established in legal doctrine and can be interpreted differently in different contexts. In a commercial law context, the term may be defined loosely as any of a variety of rights, claims and remedies that afford a person (the rightholder) control over data, including the manner in which data is processed, the purposes for which it is provided, and the outcome of that processing. Essentially, data rights are "property-like" rights that are tailored to the peculiar qualities of data as an intangible, non-rivalrous (albeit potentially excludable) commodity but without the need to recognize data as an object of property.

27. A "data right" is an abstract notion, in the sense that it requires the law to recognize its existence and to prescribe the circumstances in which the data right is vested in the rightholder, the person against whom the right may be enforced, and the mechanism for enforcement. Data rights, as defined, are already recognized under a range of laws, including laws relating to trade secrets, data privacy and database rights. In broad terms, those existing regimes afford a range of controls over how data is processed, including (i) gaining access to data, (ii) requiring a person to desist from processing data, and (iii) requiring data to be corrected or erased. Data rights are also established by contract and enforced under contract law. However, it is proposed that future work focus on data rights independent of contract, and thus unrestrained by privity of contract.

IV. Legal issues for future work on data contracts

A. Background

28. The main body of law applicable to data contracts is contract law. While contract law generally gives legal force to the terms of a contract pursuant to the principle of party autonomy, it also comprises certain rules and principles that are designed to maintain a level of fairness in commercial relations, as well as rules to fill gaps in the contract to give effect to the underlying transaction, including rules relating to sufficiency of performance and implied terms. The application of those rules to data contracts ordinarily requires consideration of the nature and purpose of the contract (i.e. the data transaction) and established commercial practice (i.e. among actors in the data ecosystem), which in turn requires an understanding of the data economy. It is worth recalling (see para. 18 above) the point stressed at the sixty-third session of Working Group IV about the complexities of the data ecosystem.

[29] Ibid., para. 16: "The various actors in an online platform are connected by a series of contractual relationships. A contract will ordinarily be concluded between the platform operator and each platform user, which incorporates the terms of use for the platform (i.e. the platform rules). The terms of the contract may vary on account of the capacity in which the user interacts through the platform, including any additional services that it uses. One or more contracts may also be concluded between users in the course of their interaction via the platform".

29. The secretariat has observed in its exploratory work that gaps exist not only in terms of the application of contract law principles to data contracts, but also in terms of the provisions to be contained in data contracts. As observed in the introductory note to the ALI/ELI Principles, uncertainty as to the applicable legal rules risks undermining predictability necessary for efficiency in data transactions. It can also inhibit innovation and growth, and lead to market failure and manifest unfairness, particularly for the weaker party in a commercial relationship.[30] Weaker parties, such as micro, small and medium-sized enterprises, are particularly prone to uncertainty with regard to the contents of data contracts, leaving them exposed to contract provision established by dominant market participants that do not protect their commercial interests.

30. Several national and transnational initiatives have sought to fill those gaps for data contracts, including the contract guidelines published by the Ministry of Economy, Trade and Industry of Japan in 2018 on the utilization of data ("METI Data Guidelines")[31] and the ALI/ELI Principles (see para. 9 above). Both of those initiatives were presented to the sixty-third session of Working Group IV and provide a source of inspiration for future work on data contracts.

B. Data provision contracts

31. The secretariat has examined the provisions of the United Nations Convention on Contracts for the International Sale of Goods[32] (CISG) as a possible source of inspiration for future work defining the contents of data provision contracts, adopting a cautious view that such contracts do not constitute a "contract for sale" and that data can be characterized as a "good".[33] The secretariat has observed that, while the provisions of the CISG are not tailored to the particular needs of the parties to data provision contracts,[34] the legal issues dealt with in those provisions – particularly the rights and obligations of the parties and remedies for breach of contract may offer a blueprint or methodology for future work on data provision contracts.

1. Rules on how data is transferred (shared) or accessed

32. Under the CISG, delivery of the goods constitutes the seller's primary obligation under a sales contract. The different rules on delivery set out in article 31 CISG could be tailored to the context of data provision contracts, in which data can be provided by different modes, including by transferring the data to an information system under the control of the recipient or by giving the recipient access to the data in a system under the control of the data provider (with or without the ability to port the data to a system under the control of the recipient). At the sixty-third session of Working Group IV, a distinction was drawn between (i) the "porting" data, by which the data recipient initiates a transfer of data from the data provider under a data provision contract, and (ii) the "portability" of data, by which data is subject to compatibility requirements under a data processing contract to facilitate the service recipient switching to another service provider.

---

[30] ALI/ELI Principles, introductory note.

[31] Japan, Ministry of Economy, Trade and Industry, *Contract Guidelines on the Utilization of AI and Data: Data Section*. An English translation of the original version of the METI Data Guidelines (June 2018) is available at www.meti.go.jp/english/press/2019/0404_001.html (accessed on 27 April 2022). The METI Data Guidelines (in the original Japanese) have since been updated following the amendments to the Unfair Competition Prevention Act outlined in para. 50 below: see www.meti.go.jp/english/press/2019/1209_005.html (accessed on 27 April 2022).

[32] United Nations, *Treaty Series*, vol. 1489, No. 25567.

[33] For a recap of those questions, see A/CN.9/1012/Add.2, paras. 42-45.

[34] The differences between data flows and cross-border trade in goods and services is highlighted by UNCTAD in the most recent Digital Economy Report; *Digital Economy Report 2021 – Cross-border Data Flows and Development: For Whom the Data Flow* (Geneva, 2021), pp. 74-76.

33. Future work could develop rules on how data is provided under a data provision contract which accommodate the different modes by which data is provided in practice. Those rules could be subject to a proviso that the mode of delivery be reasonable in the light of data security concerns.

2. Rules on data conformity

34. Article 35 CISG contains detailed rules on the conformity of goods. The primary test for conformity in article 35(1) defers to the terms of the contract itself, requiring the seller to "deliver goods which are of the quantity, quality and description required by the contract and which are contained or packaged in the manner required by the contract". Article 35(2) provides supplementary conformity rules requiring goods to be fit for their ordinary purposes, fit for their particular purposes, possess the qualities held out via any sample or model, and be packaged in their usual manner or in an adequate manner. Article 35(3) provides a safe harbour from liability under article 35(2) if "the buyer knew or could not have been unaware of such lack of conformity".

35. The elements of conformity in the CISG – quantity, quality, fitness for purpose and reference to samples and models – can readily be transposed to data and are important elements of data provision contracts, as demonstrated by the METI Data Guidelines and ALI/ELI Principles (see, e.g. principle 7(2)(b)). Already at the sixty-third session of Working Group IV, it was foreshadowed that future work could focus on assurances as to the quality of data. Moreover, the element of "packaging" (for goods) finds a ready equivalent in the structure and format in which data is provided. The examination and notice rules under articles 38 and 39 of the CISG are closely linked with the conformity rules and may also be tailored to data provision contracts.

36. Future work could develop rules on data conformity in terms of quantity, quality, fitness for purpose and format. Rules on quantity could address issues such as frequency of provision, while rules on quality could address data-specific characteristics such as accuracy and currency, as well as "traceability", which could incorporate assurances as to the origin and integrity of data.

3. Rules on the use of data by the parties

37. Article 42 CISG obliges the seller to deliver goods that are free from any right or claim of a third party based on industrial property or other intellectual property. However, the obligation does not apply if the buyer "knew or could not have been unaware of the right or claim" or if the third party right or claim results from specifications furnished by the buyer.

38. As outlined above (para. 19), rights or claims based on industrial property or other intellectual property, in particular copyright and trade secrets, control the use of data, as can rights and claims under privacy and data protection laws and laws relating to database rights. Ordinarily, the data recipient should be put in a position by the data provider to use or otherwise control the data and any derived data for the purposes of the contract free of any such rights and claims of any third party (i.e. other data rights). Already at the sixty-third session of Working Group IV, it was foreshadowed that future work could focus on assurances that the data was lawfully provided and could lawfully be processed. In that regard, it was suggested in particular that data provision contracts should include a warranty that the data provided by the data provider and that the intended use of the data by the data recipient complied with applicable laws relating to data privacy.

39. Future work could develop rules on the control and use of data under data provision contracts. In addition to the warranty suggested above (para. 38), the rules could contemplate exceptions based on the knowledge of the data recipient or compliance by the data provider with the data recipient's own specifications, inspired by article 42 CISG. Moreover, in view of the peculiar qualities of data, future work could also extend the rules to address the residual rights of the data provider to process

the data, including to retain a copy of the data and to continue using the data, and to provide the data to third parties.

4. Rules on remedies in the event of breach of contract

40. The CISG establishes a range of remedies that are available to either party in the event of breach of contract by the other party. Some of those remedies may not be suitable to data provision contracts, while others may require tailoring (e.g. the duty to make restitution). At its sixty-third session, Working Group IV did not address the issue of remedies. Future work could consider developing tailored rules on remedies for breach of data provision contracts, taking into account the peculiar qualities of data.

C. Data processing contracts

41. In its progress report to the Commission in 2021 (A/CN.9/1064, para. 21), the secretariat noted that many of the legal issues raised by data processing contract have been touched on by the secretariat in its *Notes on the Main Issues of Cloud Computing Contracts*.[35] After all, cloud computing is a type of data processing service. Building on past work of Working Group IV on the topic of cloud computing, several areas for possible harmonized rules have been identified by the secretariat.

1. Rules on data security and data integrity

42. Rules on data security and data integrity refer to the policies and procedures to maintain data security and integrity and to manage security incidents. Future work could develop rules on the standards to be maintained by the service provider under a data processing contract, including by limiting the information systems and locations in which data processing services may be provided.

2. Rules on data portability

43. As noted above (para. 32), rules on data portability are relevant to certain data provision contracts. Future work could develop rules on standards to be observed by the service provider under a data processing contract regarding the compatibility of processed data to facilitate the service recipient switching to another service provider or otherwise using the processed data.

3. Rules on the use of data by the parties

44. Future work could also develop rules limiting the use by the service provider of data provided or processed under the contract, for instance rules restricting transfers to third parties or use of the data for purposes other than the provision of the data processing services.

4. Rules on transparency

45. At the sixty-third session of Working Group IV, a view was expressed that data processing contracts should include an obligation on the service provider to disclose and explain to the service recipient how data was being processed under the contract. It was observed, however, that transparency with respect to the processing of data should pay due regard to copyright and trade secrets, particularly given the use of proprietary methods to process data. Future work could develop rules that balance those needs.

[35] *Notes on the Main Issues of Cloud Computing Contracts*, available at https://uncitral.un.org/cloud.

V. Legal issues for future work on data rights

A. Background

46. The data ecosystem involves multiple actors who are not always in a contractual relationship with one another. Yet despite the focus on data governance and cross-border data flows, there is currently no coherent legal regime that specifically recognizes the control that actors in the data ecosystem may legitimately expect to have with respect to the data that they have processed (including generated) as it is processed further down the data value chain by other actors with whom they may have no contractual relationship. Data rights recognized under existing laws exist independently of one another and pursue different policy objectives within their respective field of application. This results in a "patchwork" of rights and thus the emergence of gaps in legal protection. Those gaps can generate legal uncertainty, which may in turn inhibit data transactions. At the sixty-third session of Working Group IV, it was acknowledged that the absence of legal recognition of data rights was a source of legal uncertainty in some jurisdictions.

47. Against this background, a key legal issue that frequently arises is data ownership, which the secretariat has explored in A/CN.9/1012/Add.2 (paras. 22–32). A survey of case law and commentary in a variety of jurisdictions suggests that data is not – and should not be – an object of property rights, not only in view of its peculiar qualities, but also due to concerns that vesting property rights in data could ultimately harm data flows, limit business opportunities in the data economy, and harm the overall integrity of the existing property law regime. At the sixty-third session of Working Group IV, broad support was expressed for future work not to consider data as an object of property rights.

48. Proposals to fill those gaps have therefore turned to identifying a new "bundle" of data rights, independent of contractual relations and property law, that allows upstream actors to control – and possibly draw benefits from – the downstream processing of data. This chapter outlines how a legal framework of sui generis property-like rights in data with third party effect could be developed.[36]

B. Relevant initiatives

49. At its sixty-third session, Working Group IV heard of several initiatives related to data rights, including recent legislative reforms in Japan and the Republic of Korea and the provisions of the ALI/ELI Principles dealing with data rights.

50. In Japan, the Unfair Competition Prevention Act was amended in 2018 to introduce provisions on unfair competition related to data with a view to promoting a business environment that "rewards the efforts of data creators, collectors, analysers, and controllers".[37] The provisions apply to "shared data with limited access", which is defined to comprise technical or business data that is provided by the data holder to specified persons on a regular basis, for example market analysis data, operational data, and data relevant to an ongoing business relationship (e.g. under a franchise or joint venture arrangement). As amended, the Unfair Competition Prevention Act prescribes a range of acts related to such data, which can broadly be divided into three categories, namely: (i) wrongful acquisition from the data holder; (ii) use or disclosure in circumstances constituting a significant breach of good faith toward the

[36] In its 2021 World Development Report, the World Bank posits that data requires a normative framework that "ensure[s] and promote[s] trust in the data governance and data management ecosystem by avoiding and limiting harm arising from the misuse of data or breaches affecting their security and integrity" while also "facilitat[ing] the use, reuse, and sharing of data within and between stakeholder groups through openness, interoperability, and portability": *Data for Better Lives* (Washington, 2021), p. 191.

[37] See Ministry of Economy, Trade and Industry, *Guidelines on Shared Data with Limited Access* (23 January 2019), pp. 3–5.

data holder; and (iii) subsequent acquisition or disclosure of data with knowledge of its wrongful acquisition or improper disclosure. Existing civil remedies under the Unfair Competition Prevention Act, including injunctions and claims for damages, are available to the data holder. Significantly, except for the second category, which presupposes an agreement akin to a data provision or data processing contract, unfair competition related to "shared data with limited access" does not presuppose the existence of a contractual relationship between the data holder and the wrongdoer. As such, the remedies available to the data holder may be likened to a form of "data rights" (as described in para. 27 above).

51. In the Republic of Korea, the Unfair Competition Prevention and Trade Secret Protection Act was amended in 2021 to clarify how the unfair competition regime applies to data that is provided in the course of business, in particular data that is not otherwise subject to protections related to trade secrets, copyright and database rights. As amended, the Act defines each of the following as an "act of unfair competition": (i) unauthorized acquisition and use of data; (ii) use of data in circumstances constituting a breach of good faith; and (iii) the subsequent acquisition of data with knowledge of its unauthorized acquisition. Among other things, an act of unfair competition with respect to data is subject to civil remedies under the Act including injunctions and claims for damages.

52. The ALI/ELI Principles provide an alternative approach to the extracontractual control over the use and disclosure of data by downstream actors. In a practice sometimes referred to as "leapfrogging", which is already known to some legal systems with respect to value chain contracts, the ALI/ELI Principles recognize the right of an initial data provider to control downstream processing of data beyond the immediate recipient of the data if (i) the immediate recipient provided the data to the downstream recipient in line with contractual terms agreed with the initial data provider, (ii) those contractual terms required the immediate recipient to impose terms of use on the downstream recipient, and (iii) the downstream recipient breached those terms. While the ALI/ELI Principles do not prescribe remedies, requiring the downstream recipient to desist from processing the data, requiring the data to be corrected or erased, or claiming damages could be envisaged.

53. The legislative reforms in Japan and the Republic of Korea and the "leapfrogging" provisions of the ALI/ELI Principles exhibit common elements both in terms of their objectives and the data rights that they recognize, and provide a source of inspiration for future work on data rights. Those data rights are by no means exhaustive. For example, the ALI/ELI Principles also recognize rights in "co-generated data", which are vested in the person who had a significant role in the generation of the data, thus reflecting the policy that "whoever has contributed to the generation of data should generally have some rights with respect to its use or with respect to the value it generates".[38] The content of rights in co-generated data is not fixed by the ALI/ELI Principles, but depends on the circumstances surrounding the generation of data. For example, it could extend to the rightholder gaining access to the data, requiring a person to desist from processing the data, or requiring the data to be corrected or erased. In exceptional circumstances, the rightholder might also have a claim to an economic share in profits derived from the use of the data.

54. At the sixty-third session of Working Group IV, support was expressed for focusing on co-generated data as a starting point for possible future work on data rights. Interest was also expressed in the initiatives outlined above (paras. 50-52) that are aimed at allowing upstream actors to control the downstream use and disclosure of data. However, some doubts were expressed about building consensus around identifying the class of rightsholders and the content of data rights in general. Further preparatory work could be done to clarify those matters. Moreover, preliminary investigations by the secretariat have identified initiatives to recognize data rights in other circumstances that exhibit common elements with other national legislative initiatives on which harmonized rules could be developed. An example is again

[38] ALI/ELI Principles, p. 28.

provided by the ALI/ELI Principles, which recognize certain data rights that are for the public interest.

VI. Proposal

55. The Commission may wish to recall the view, expressed at the fifty-fourth session, that the topic of data transactions might eventually be referred to Working Group IV to be dealt with in tandem with the topic of the use of automated contracting. Subject, therefore, to its deliberations on the future work of the Working Group on the topic of automated contracting (see A/CN.9/1116, chap. II), the Commission may wish to consider mandating the Working Group to proceed with work on data contracts as outlined in this note.

56. In that regard, it may wish to invite the Working Group to focus on data provision contracts in the first instance, in line with the preference that emerged at the sixty-third session of the Working Group. The Commission may also wish to invite the Working Group to keep data processing contracting under consideration and to report back to the Commission at a later session on how they could be dealt with in future work. As the secretariat noted in its progress report to the Commission in 2021 (A/CN.9/1064, para. 23), it is possible that work on data provision contracts will inform further consideration of data processing contracts and identify commonalities between the two types of contracts. The Commission may wish to defer any decision as to the form of future work on data contracts. In that regard, several options were already canvassed at the sixty-third session of the Working Group, including the development of “default” rules to be included in a legislative text, a guide to good practice for parties, or a legislative guide.

57. As for data rights, the Commission may wish to consider mandating the secretariat to continue preparatory work on data rights as outlined in this note. Specifically, it may wish to request the secretariat (a) to study other initiatives related to data rights with a view to mapping the classes of rightsholders and the content of the data rights recognized, and to identifying common elements on which harmonized rules could be developed, and (b) to report back to the Commission at a later session.