United Nations A/CN.9/1012/Add.2

General Assembly

Distr.: General
12 May 2020

Original: English

**United Nations Commission on International Trade Law**
**Fifty -third session**
New York, 6–17 July 2020

# Legal issues related to the digital economy – data transactions

## Contents



V.20-02554 (E) 150520 180520

# I. Context

1. As noted in A/CN.9/1012, by one forecast, the amount of data created each year is projected to increase from approximately 16 trillion gigabytes to 163 trillion gigabytes by 2025.[1] In its 2019 *Digital Economy Report*, the United Nations Conference on Trade and Development (UNCTAD) describes a "data economy", created by the importance of data in driving economic development, and featuring a "data market" for a range of data-related services. In the European Union (EU) alone, the value of the data economy (i.e., the impact of the data market on the overall economy) is estimated to be 477 billion euros in 2020.[2]

2. In the data economy, data transactions occur along a "data value chain", which produces "digital intelligence" that can be used to inform decision-making and develop new products.[3] Different types of data are transacted at different stages along this chain. While raw data at one end of the chain has limited scope to generate value alone, "derived data" (i.e., data that is created through processing of raw data) and "aggregated data" (i.e., a combined dataset made up of various data sources) generated along the chain have significant potential.

3. Data value chains exist not only at the national level but also the international level. Cross-border data flows are particularly relevant for international trade and development. As noted by UNCTAD, "[t]he global reach of global digital platforms, and the fact that they are driven by data, results in massive amounts of data flowing internationally between users and platforms located in different countries".[4]

4. Given the importance of data to international trade, it is important to assess the application of existing trade-related laws to data transactions and to other uses of data in trade. Among other things, this paper does not address privacy and data protection laws (noting that these matters give rise to sensitive public policy issues),[5] nor does it address intellectual property law.

# II. What is data and what are data transactions?

5. According to the well-recognized definition formulated by the International Organization for Standardization (ISO), "data" is "a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing".[6] A similar understanding of data – as a representation of information – underlies the notion of "data message" in UNCITRAL texts on electronic commerce, which is defined as "information generated, sent, received or stored by electronic, magnetic, optical or similar means".[7] On the basis of the ISO definition, data need not be in electronic or machine-readable form, although such data offers greater potential value in the digital economy.[8]

6. As part of an ongoing joint project to develop principles for a data economy (discussed further at paragraph 15 below), the American Law Institute (ALI) and the European Law Institute (ELI) are examining legal rules that are applicable to data

[1] World Trade Organization, *World Trade Report 2018: The Future of World Trade* (Geneva, 2018), p. 28.

[2] European Data Market Monitoring Tool, available at http://datalandscape.eu/european-data-market-monitoring-tool-2018.

[3] UNCTAD, *Digital Economy Report 2019 – Value Creation and Capture: Implications for Developing Countries* (Geneva, 2019), p. 29.

[4] Ibid, p. 89.

[5] At its fifty-first session, the Commission decided that the exploratory work of the Secretariat should "avoid privacy and data protection issues": *Official Records of the General Assembly, Seventy-third Session, Supplement No. 17* (A/73/17), para. 253(b).

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

[7] UNCITRAL Model Law on Electronic Commerce, art. 2(a); United Nations Convention on the Use of Electronic Communications in International Contracts, art. 4(c). In the UNCITRAL Model Law on Electronic Transferable Records, the term "electronic record" is used.

[8] 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".

transactions, with a view to developing principles for a data economy (hereafter the "ALI/ELI Principles").[9] According to the current draft of the ALI/ELI Principles, a "data transaction" means "a transaction with regard to the control or processing of data, or to any rights with regard to the data",[10] whereby "control" is defined as the ability to access data and to determine the purposes and means of its processing (with or without having a right to do so) and "processing" is defined to include operations such as recording, organizing, structuring, storage, adaptation or alteration, retrieval, transmission, alignment or combination, restriction, erasure or destruction of data.

7. The current draft ALI/ELI Principles makes special provision for the following types of data transactions:

(a) transferring data;

(b) providing or permitting access to data or a data source;

(c) sharing data on an online platform;

(d) providing data processing services; and

(e) providing services to facilitate data transactions (including via an online platform).

8. In order to clarify certain matters relating to data transactions, the Ministry of Economy, Trade and Industry of Japan published in 2018 the Contract Guidelines on the Utilization of AI and Data: Data Section (hereafter the "METI Data Guidelines"),[11] with a view to "promoting reasonable negotiations and execution of contracts, reducing transaction costs and diffusing data contracts". Unlike the ALI/ELI Principles, the METI Data Guidelines treat data generation as a separate type of data transaction.

9. As noted by UNCTAD, the various types of data being transacted in the data economy may be classified according to a range of different criteria, including: personal or non-personal data; private or public data; data for commercial purposes or governmental purposes; data used by companies, including corporate data, human resources data, technical data or merchant data; structured or non-structured data; instant or historic data; volunteered, observed and inferred data;[12] sensitive or non-sensitive data; and business-to-business (B2B), business-to-consumer (B2C), government-to-consumer (G2C) or consumer-to-consumer (C2C) data.[13] These classifications indicate that data and data transactions potentially engage a wide range of stakeholders as well as a wide range of laws.

[9] For information on this joint initiative, see www.europeanlawinstitute.eu/projects-publications/current-projects-feasibility-studies-and-other-activities/current-projects/data-economy/.

[10] The draft ALI/ELI Principles are currently in the form of ALI Council Draft No. 1 (8 December 2019), on file with the Secretariat.

[11] Japan, Ministry of Economy, Trade and Industry, *Contract Guidelines on Utilization of AI and Data: Data Section* (June 2018), English translation available at www.meti.go.jp/press/2019/04/20190404001/20190404001-1.pdf.

[12] According to a paper published by the World Economic Forum, "volunteered data" (i.e., data created and explicitly shared by individuals such as social network profiles), "observed data" (i.e., data captured by recording the actions of individuals such as location data when using cell phones) and "inferred data" (i.e., data about individuals based on analysis of volunteered or observed information such as credit scores) are three categories of personal data. See *Rethinking Personal Data: A New Lens for Strengthening Trust* (Geneva, 2014), pp. 16–17.

[13] UNCTAD, *Digital Economy Report 2019*, p. 29. Several of these criteria are primarily concerned with personal data (i.e., data related to an identified or identifiable individual).

# III. Actors

10. The data value chain involves not only a range of different stages in the control and processing of data but also a range of different actors. These different actors may be defined by the functions that they perform along the data value chain, including:

(a) The data generator (i.e., the person who generates data, including by way of a machine or sensor, as well as data that is generated from other data);

(b) The data subject (i.e., the person to whom data relates);

(c) The data provider (i.e., the person who provides data, including a person who provides data that is shared on an online platform);

(d) The data recipient (i.e., the person who receives data, including a person who gains access to data that is shared on an online platform);

(e) The data processor (i.e., the person who processes data, regardless of whether the person generates or receives the data); and

(f) The data platform operator (i.e., the person who hosts data on an online platform).

# IV. Legal regimes

11. This section addresses two aspects of data transactions, as defined above (para. 6), namely (a) the rights and obligations of parties to data transactions, and (b) data as a commodity.

## A. Rights and obligations of parties to data transactions

### 1. Contract law

12. Insofar as data transactions are contract-based, the main body of law applicable to data transactions is contract law. To assist in understanding the types of contractual rights and obligations at stake, data transactions may be categorized into the following three types of contract:

(a) *Data provision contracts* – this type of contract deals with transactions in which the data provider provides data or access to data to the data recipient, and generally sets out the data recipient's usage rights and other conditions of the data provision. The contract may provide for the data provider to relinquish its control over the data, in which case the transaction may be likened to an "assignment" of data. Alternatively, it may provide for the data provider to retain its usage rights.

(b) *Data generation contracts* – this type of contract establishes usage rights between the parties in newly generated data (e.g., raw data produced by sensors and data derived therefrom through processing, analysis, editing, and integration).[14] The parties may also agree on warranty over content and continuous generation of data, distribution of profits and expenses, as well as data management and security-related issues.[15]

(c) *Data-related service contracts* – this type of contract deals with the provision of data processing services under which one party is obliged to process data provided by the other party and grant the other party access to the processed data. This includes the provision of data scraping services, cloud-based services,[16] data analytics, data platform services, and electronic transmission services. These

[14] METI Data Guidelines, p. 5.

[15] Ibid., p. 42.

[16] The Secretariat has recently published its *Notes on the Main Issues of Cloud Computing Contracts*, available at https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-09103_eng.pdf.

contracts also deal with the provision of services by an intermediary to facilitate data transactions (including via an online platform).

13. A report prepared by the Support Centre for Data Sharing initiative funded by the European Commission found that model contract terms used by industry stakeholders generally include provisions relating to (i) the content or nature of the data (e.g., personal data, public sector information, confidential information), (ii) commercial/business terms (e.g., remuneration, contract duration, termination for cause), (iii) control, "ownership" and usage rights (e.g., exclusive control, intellectual property rights, restrictions), (iv) general legal context (e.g., applicable law, dispute resolution), and (v) the service providing the data (e.g., availability, response time).[17]

14. Whereas 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 the level of fairness in commercial relations that each legal system considers desirable. In the context of data transactions, there appears to be uncertainty not only between parties as to the rights and obligations to be embodied in their contracts, but also on the part of lawyers and judges as to the application of existing rules and principles of contract law. For example, contract law rules relating to sufficiency of performance and implied obligations, such as those relating to the mode of supply and quality of data, might require consideration of the nature and purpose of the contract (i.e., the data transaction) and established commercial practice (i.e., among participants in the data market), which in turn requires an understanding of the emerging data economy.

15. This uncertainty has motivated several initiatives in recent years, notably the publication of the METI Data Guidelines, the establishment of a Code of Conduct on Agricultural Data Sharing by Contractual Agreement between members of the agricultural industry in the EU, and the development of the ALI/ELI Principles (which are due to be finalized in 2021). As noted on the webpage of the joint ALI/ELI project:

> Both in the US and in Europe, the data economy is beginning to trouble stakeholders, such as consumers, data-driven industries, and start-ups, because there is uncertainty as to the applicable legal rules and doctrines. Concerns range from manifest uncertainty of the law, potentially inhibiting innovation and growth, to a loss of control by governments, legislatures and judiciaries, to serious issues of consumer protection and fundamental rights. More fundamentally, there is already uncertainty about what rights parties 'own' and can trade in, e.g., who 'owns' the data generated by an activity such as driving a connected car, what are the attributes of that data and rights related to it, and who might have to pay compensation to whom for exploiting the data's economic potential. This uncertainty undermines the predictability necessary for transactions in data and has resulted in lawmakers and the courts grappling with these issues.

### 2. Sales of goods law

16. In many jurisdictions, contract law is supplemented by specific sale of goods legislation. In some of these jurisdictions, the notion of "goods" refers only to tangible things. In other regimes, however, the notion of "goods" is broader. Moreover, the term "sale" generally involves the transfer of property rights (discussed below).[18]

17. Sale of goods legislation in many common law jurisdictions is based on the (now repealed) *Sale of Goods Act 1893* of the United Kingdom. Courts in some of these jurisdictions have found that the legislation does not apply to software, let alone data.[19] While legislative reform in countries like New Zealand has expanded the

[17] *Support Centre for Data Sharing Report: Collected Model Contract Terms* (July 2019), pp. 6–7.

[18] See the "commonly accepted definition" articulated by the Court of Justice of the European Union in *UsedSoft GmbH v. Oracle International Corp*, discussed in para. 28 below.

[19] In the United Kingdom, with respect to the *Sale of Goods Act 1979*, see Court of Appeal of England and Wales, *St. Albans City and District Council v. International Computers Limited*,

legislation to cover software,[20] it seems unlikely that it would apply to data generally. In the United States of America, the Uniform Commercial Code does not specifically address software transactions but some courts have chosen to apply it to such transactions.[21] It is worth mentioning that the Uniform Computer Information Transactions Act[22] has been proposed as model rules for state legislatures to adopt to regulate transactions in computer information products such as computer software and online databases; however, it has not been widely adopted.

18. In civil law jurisdictions such as Germany, pursuant to section 453 of the Civil Code, provisions on the sale of goods apply equally to rights and other objects, which may include data. In France, sales concern the delivery of a "thing" under article 1582 of the French Civil Code, which does not include data. In China, pursuant to article 132 of the Contract Law, provisions concerning sales contracts apply to any subject matter owned by the seller or of which the seller has the right to dispose. In Japan, based on article 555 of the Civil Code, sales contracts involve the transfer of certain real rights, which are the rights to derive ownership interests and benefits with respect to the subject matter of the sale. Arguably in China and Japan, the existing sales of goods provisions may apply to data provided that rights similar to ownership over data would be recognized (see discussion below on property rights in data).

### 3. Other regimes

19. In 2018, the EU adopted a framework regulation for the free flow of non-personal data.[23] Among other things, the regulation provides for the development of industry codes of conduct for data portability, with a particular focus on cloud-based service providers, with the aim of avoiding so-called "vendor lock-in practices" and encouraging competition in the data market. While not legally binding, these codes of conduct have the effect of imposing additional requirements on data-related service providers, such as disclosure requirements and requirements to facilitate the switching of service providers by users.[24]

## B. Data as a commodity

20. The various actors along the data value chain will not always be in a contractual relationship with one another. Accordingly, there are limits to which an actor can avail itself of contract law to protect its interests in data where the data is utilized by a third party (e.g., under the doctrine of privity of contract in common law jurisdictions).

21. This section analyses legal regimes applicable to data as a commodity, namely (i) property law, and (ii) other regimes including criminal law.

---

Case No. QBENF 94/1521/C, Judgment, 26 July 1996, *All England Law Reports*, vol. 1996, No. 4; Court of Appeal of England and Wales, *Computer Associates UK Limited v Software Incubator Limited*, Case No. A3/2016/3823, Judgment, 19 March 2018, *Lloyd's Law Reports*, vol. 2018, No. 1, [2018] EWCA Civ. 518. In Australia, with respect to the *Sale of Goods Act 1923* of the state of New South Wales, see New South Wales Supreme Court, *Gammasonics Institute for Medical Research Pty. Ltd. v. Comrad Medical Systems Pty. Ltd.*, Case No. 2009/14136, Judgment, 9 April 2010, *New South Wales Law Reports*, vol. 77, p. 479, [2010] NSWSC 267.

[20] See *Sale of Goods Amendment Act 2003*, section 3, which amendment is now reflected in the *Contract and Commercial Law Act 2017*, section 119(1).

[21] See, e.g., Civil Court of the City of New York, *Communications Groups, Inc. v. Warner Communications, Inc.*, Judgment, 28 March 1988, *New York Miscellaneous Reports, Third Series*, vol. 138, p. 80.

[22] National Conference of Commissioners on Uniform State Laws, Uniform Computer Information Transactions Act (2002), available at www.uniformlaws.org/viewdocument/committee-archive-52?CommunityKey=92b2978d-585f-4ab6-b8a1-53860fbb43b5&tab=librarydocuments.

[23] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union.

[24] See SWIPO, "Multi-Stakeholder Group Presents Codes of Conduct to Enable Competition and Data Portability for Cloud Service Customers Across Europe", press release, Helsinki, 26 November 2019, available at www.swipo.eu/media/SWIPO_press_release.pdf.

### 1. Property law

22. At present, most legal systems appear not to regard data as an object of property rights. For example, data is not included as an object of property rights in the civil codes of Argentina,[25] France,[26] Japan,[27] the Russian Federation[28] or Spain.[29]

23. In Germany, it has been recognized by several courts that data is not a "thing" under section 90 of the Civil Code and therefore not subject to conventional ownership rights, which are reserved for physical objects.[30] However, the deletion of data saved on a hard disk has been considered to be a violation of "property" ("*Eigentum*") in the hard disk for the purposes of a claim for damages under section 823 of the Civil Code.[31]

24. In China, article 127 of the General Provisions of the Civil Law signals that data may be protected by law but does not expressly recognize it as an object of property rights. Rather, it merely mentions that "[w]here any laws provide for the protection of data … such laws shall apply". In a 2018 judgment, a first instance court in Hangzhou recognized rights and interests in big data products claimed by a network operator from the perspective of competition law in order to protect the network operator's investment in such products. However, in the absence of any existing legislation dealing with rights over data products, the court refused to recognize ownership over the data products, noting that ownership was an absolute right and, if granted to network operators, corresponding obligations would be imposed on an unspecified majority of the population.[32] This finding was confirmed in 2019 by the Zhejiang Higher People's Court, which described the rights and interests in the data products as "competitive property rights and interests".[33]

25. In England, where "the law has been reluctant to treat information itself as property", the Court of Appeal recently confirmed in the case of *Your Response Ltd. v. Datateam Business Media Ltd.* that data in an electronic database was not tangible property for the purposes of English common law and therefore that: (a) data was not capable of being the subject of a possessory lien (i.e., the right of a bailee to refuse to return property); and (b) withholding data could not be the subject of a claim for conversion (i.e., a claim for the wrongful interference with property).[34] The court did, however, concede that there was a "powerful case" for recognizing intangible things such as digitized materials as a new category of property, but added that this legal development would require "the intervention of Parliament".[35]

26. The courts in Australia have taken a similar approach.[36] The courts in New Zealand, however, have shown a greater willingness to extend the categories of property at common law into the digital realm without legislative intervention. For instance, in the case of *Henderson v. Walker*, the High Court accepted that the plaintiff's digital files were capable of possession and therefore that interference with

[25] Articles 15 and 16.
[26] Article 544.
[27] Articles 85 and 206.
[28] Article 128.
[29] Article 348.
[30] See, e.g., Regional Court, Constance, Case No. 1 S 292/95, Judgment, 10 May 1996; Higher Regional Court, Dresden, Case No. 4 W 961/12, Judgment, 5 September 2012.
[31] Higher Regional Court, Karlsruhe, Case No. 3 U 15/95, Judgment, 7 November 1995; see also Higher Regional Court, Oldenburg, Case No. 2 U 98/11, Judgment, 24 November 2011.
[32] Hangzhou Railway Transportation Court, *Taobao (China) Software Co., Ltd. v. Anhui Meijing Information Technology Co., Ltd.*, Zhe 8601 Min Chu No. 4034, Judgment, 16 August 2018.
[33] Zhejiang High People's Court, *Anhui Meijing Information Technology Co., Ltd. v. Taobao (China) Software Co., Ltd.*, Zhe Min Shen No. 1209, Judgment, 2 July 2019.
[34] *Your Response v. Datateam Business Media,* Case No. B2/2013/1812, Judgment, 14 March 2014, *Official Law Reports: Queen's Bench Division*, vol. 2015, p. 41, [2014] EWCA Civ 281.
[35] Ibid, para. 27.
[36] *See New South Wales Supreme Court, Hoath v. Connect Internet Services, Case No*. 1599/02, Judgments, 22 March 2006, *Australian Law Reports*, vol. 229, p. 566 [2006] NSWSC 158.

those files could give rise to a claim for conversion.[37] The court added that this applied to all "digital assets", which it defined to include "all forms of information stored digitally on an electronic device, such as emails, digital files, digital footage and computer programmes" (note that these are not the same types of digital assets that are the focus of addendum 3).[38] It is not clear whether this case represents authority that *all* data, regardless of how it is structured, would be protected by a claim for conversion, although a subsequent judgment of the High Court has stated that the case extends the claim "to purely digital information".[39]

27. In the United States of America, it has been accepted in some states that a claim for conversion extends to intangible objects.[40] For instance, in the case of *Thyroff v. Nationwide Mutual Insurance Co.*, the Court of Appeals of the state of New York held that a claim for conversion under the law of that state extended to "electronic records that were stored on a computer and were indistinguishable from printed documents", which in that case comprised customer and personal information stored in a principal's computer system accessible by an agent through a licensed computer.[41] The court nevertheless cautioned that it did not consider "whether any of the myriad other forms of virtual information should be protected by the tort".[42]

28. In the EU, some legal commentators have found that the Court of Justice, in the case of *UsedSoft GmbH v. Oracle International Corp.*, opened the door for a discussion on ownership in intangible objects.[43] In that case, the court held that the commercial distribution of software by internet download could constitute a sale for the purposes of Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs. In reaching that conclusion, the court found that, according to a commonly accepted definition, a "sale" was an agreement by which "rights of ownership in an item of tangible or intangible property belonging to [one person]" are transferred to another person in return for payment, and reasoned that, therefore, a "commercial transaction giving rise … to exhaustion of the right of distribution of a copy of a computer program must involve a transfer of the right of ownership in that copy".[44] The applicability of that decision to other digital goods and in other areas of EU law remains to be considered.

29. Treating data as property raises a range of legal and public policy issues. Some of these policy issues were assessed by the High Court of New Zealand in *Henderson v. Walker* in considering extending the claim for conversion to "all forms of information stored digitally on an electronic device", which the court referred to as "digital assets":

> There are also very good policy reasons for extending the tort of conversion to digital assets. Currently the (civil) law offers protection where the tangible asset containing the digital assets is converted; where the information recorded on the digital asset is obtained in breach of confidence or privacy; or where the digital asset is subject to contract, copyright or a patent. However, it would be possible to acquire digital assets in circumstances where those protections do not apply, such as if a hacker remotely deleted a non-confidential, but valuable, computer programme from a company's servers.

[37] *Henderson v. Walker*, Case No. CIV-2014-409-45, Judgment, 3 September 2019, [2019] NZHC 2184.
[38] Ibid, para. 263.
[39] *Ruscoe v. Cryptopia Limited (in liquidation)*, Case No. CIV-2019-409-000544, Judgment, 8 April 2020, [2020] NZHC 728, para. 91.
[40] *Kremen v. Cohen.*, Case No. 01-15899, Judgment, 25 July 2003, *Federal Reporter, Third Series*, vol. 337, p. 1024, [2003] USCA9 49.
[41] *Thyroff v. Nationwide Mutual Insurance Co.*, Judgment, 22 March 2007, *New York Reports, Third Series*, vol. 8, pp. 292–3.
[42] Ibid., p. 293.
[43] Case No. C-128/11, Judgment, 3 July 2012.
[44] Ibid., para. 42.

> Digital assets can have immense commercial value in the modern world, which means there is an important economic reason to ensure the law provides adequate protection for such assets.
>
> …
>
> Standing back, it seems obvious that digital assets should be afforded the protection of property law. They have all the characteristics of property and the conceptual difficulties appear to arise predominantly from the historical origins of our law of tangible property. There is a real difference between digital assets and the information they record. Such permanent records of information are already convertible when they take a physical form and it would be arbitrary to base the law on the form of the medium, especially now that digital media has assumed a ubiquitous role in modern life.

30. At the same time, the court acknowledged that there were opposing views:

> Those who oppose the extension express their concern with how the concept of possession can be applied to intangible property… Opponents point out that the common law does not give despotic control over anything with economic value, as even tangible property does not attract protection against ephemeral interferences such as visual trespass, and it is the concept of possession that provides the limitation in the case of tangible property.
>
> Opponents also point out that the common law has carefully developed categories of conversion (physical taking, detention and refusal to return, misusing and transfer to another) that are based on the physical nature of the goods. They argue that because conversion is a strict liability tort, the consequences of extending the tort into uncertain territory could be detrimental.

31. Some of the public policy considerations have been assessed within the Organization for Economic Co-operation and Development (OECD). For instance, the Trade Union Advisory Committee has published an analysis of key issues and recommendations regarding the continuing growth of the digital economy. The Committee addresses data governance and notes the importance of creating better data governance regimes and legal rules. To that end, it recommends setting "standards on data ownership including the right to access, process, and deletion, and on the pricing of data".[45] The secretariat of the OECD has also published a report on key issues for digital transformation in the G20 in which it notes that one of the challenges to encouraging investment in and sharing data is data ownership. At the same time, it notes that conferring ownership rights in data presents additional challenges in view of the range of stakeholders and range of rights that they may seek to protect, such as "the ability to access, create, modify, package, derive benefit from, sell or remove data, but also the right to assign these access privileges to others".[46]

32. Moreover, in a 2018 communication on establishing a common data space in the EU, the European Commission reported that, as regards business-to-business data sharing, stakeholders "do not favour a new 'data ownership' type of right", on the basis that "the crucial question in business-to-business sharing is not so much about ownership, but about how access is organized".[47] This seems to reflect the prevailing view in legal commentary, at least so far as unstructured data is concerned. In this regard, the "non-rivalrous" nature of data (in the sense that the use of data by one person does not limit its use by another person due to the ease with which data can be replicated) is often put forward as a reason not to make data an object of property rights, as well as the difficulty to single out the specific data that is the object of property rights. Another point made is that it is unhelpful simply to characterize data as "property" without first enquiring as to the legislative context for which the

[45] Trade Union Advisory Committee, "Digitalization and the Digital Economy: Trade Union Key Messages", February 2017, p.5.

[46] OECD, "Key Issues for Digital Transformation in the G20", report prepared for a joint G20 German Presidency/OECD conference, Berlin, 12 January 2017, pp. 65–66.

[47] Document COM (2018) 232 final 9.

characterization is needed,[48] and the implications that such characterization may have for other contexts.

### 2. Other regimes

33. Some legal regimes provide additional "layers" of protection with respect to certain types of data or representations of data. For instance, laws in many jurisdictions confer rights such as copyright, database rights,[49] rights with respect to personal data and rights (or corresponding obligations) with respect to trade secrets and confidential information. The implications of the data economy for existing intellectual property law regimes is a matter currently being considered by the secretariat of the World Intellectual Property Organization.[50] Moreover, privacy and data protection issues have been expressly excluded from the mandate given to the Secretariat.

34. In some jurisdictions, legislation has been introduced to provide some rights in data held by a third party in the event of insolvency. One example is Luxembourg, where the Commercial Code was amended in 2013 to allow data provided to be retrieved from an insolvent cloud service provider.[51] In other jurisdictions, legislation has been introduced to provide some rights to access data held by a third party in the event of death or incapacity.[52]

35. Further protection may be provided in some jurisdictions by criminal law. For instance, in Germany, section 303a of the Criminal Code criminalizes the manipulation (including deletion) of data that is subject to third party rights (section 303a German Criminal Code). In analysing whether a third party right exists, the Court of Appeal of Nuremberg has stated that the power of disposal over data in principle belongs to the originator of the recording of the data.[53] In France, the Court of Cassation ruled in a 2015 judgment that downloading data from a non-public website in order to save it on personal data carriers and distribute it to third parties could constitute theft.[54] While in New Zealand, the Supreme Court found in a 2015 judgment that digital footage was "property" within the meaning of the *Crimes Act 1967*, and therefore that obtaining digital footage from a CCTV system could constitute the crime of accessing a computer system for dishonest purposes under section 249 of the Act.[55]

36. Some legal regimes may also serve to protect data by restricting access or localization. In a cross-border context, in addition to privacy, the law may restrict the flow of data to meet other regulatory objectives such as access to information for audit purposes.[56] It may also do so to address national security concerns or to help

---

[48] Supreme Court of New Zealand, *Dixon v. The Queen*, Case No. SC 82/2014, Judgment, 20 October 2015, *New Zealand Law Reports*, vol. 2016, No. 1, p. 678, [2015] NZSC 147.

[49] See, e.g., Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases.

[50] See, WIPO, "Intellectual Property in a Data-Driven World", *WIPO Magazine*, vol. 2019, No. 5 (October 2019).

[51] Luxembourg, Law of 9 July 2013 modifying article 567 of the Commercial Code, *Official Gazette of the Grand Duchy of Luxembourg*, vol. 2577, No. 124 (18 July 2013), p. 2578.

[52] See, e.g., National Conference of Commissioners on Uniform State Laws, *Revised Uniform Fiduciary Access to Digital Assets Act (2015) with Prefatory Note and Comments*, available at www.uniformlaws.org/viewdocument/final-act-with-comments-40?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22&tab=librarydocuments, which has been enacted in almost all US states. See also Uniform Law Conference of Canada, *Uniform Access to Digital Assets by Fiduciaries Act (2016)*, available at www.ulcc.ca/images/stories/2016_pdf_en/2016ulcc0006.pdf.

[53] Higher Regional Court of Nuremberg, Case No. 1 Ws 445/12, Judgment, 23 January 2013.

[54] Court of Cassation, Criminal Division, Appeal No. 14-81336, Judgment, 20 May 2015, *Bulletin Criminel*, vol. 2015, No. 119.

[55] *Dixon v. The Queen*.

[56] Francesca Casalini and Javier López González, "Trade and Cross-Border Data Flows", OECD Trade Policy Papers, No. 220 (Paris, 23 January 2019), p. 5. For early international normative regimes responding to the automation of data processing, see OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows or Personal Data (1980), document C(80)58/FINAL, and the Convention for the Protection of

develop domestic capacity in digitally intensive sectors.[57] Cross-border data flows and data localization are issues that are currently being discussed in other international forums, including among members of the World Trade Organization as part of the Joint Statement Initiative on E-Commerce.

37. Overall, it would appear that these other regimes provide only a patchwork of coverage for actors seeking to protect their interests in data. In particular, intellectual property and similar regimes only offer protection for certain types of data or certain data-related processes, while other laws only apply in certain circumstances (e.g., insolvency) or to certain conduct (e.g., cross-border transfer of data in breach of data localization requirements). Moreover, the pursuit of remedies through the criminal justice system would ordinarily be outside the direct control of a commercial party.

38. One option to enhance legal certainty and predictability for data transactions, without expanding existing notions of property law, could be for the law to recognize a "bundle" of sui generis rights in data with third party effect. For instance, work on the ALI/ELI Principles is developing two rights that may be enforced against another person without a direct contractual relationship, namely:

(a) "Leapfrogging", by which a data provider has a right to require a downstream recipient of data to comply with terms of use, despite there being no contractual relationship between the data provider and downstream recipient, if (a) the intermediate recipient passed the data on to the downstream recipient in line with contractual terms agreed with the data provider, (b) those contractual terms required the intermediate recipient to impose the terms of use on the downstream recipient, and (c) the downstream recipient breached the terms;[58] and

(b) Rights with respect to co-generated data, by which a person who had a share in the generation of data has certain property-like rights against a data processor with respect to that data, including rights relating to (i) access to, extraction or porting of data, (ii) desistance from control and/or processing of data, (iii) correction of data, and (iv) economic share.[59] These rights bear some resemblance to rights regarding personal data under privacy laws.

39. The ALI/ELI Principles have also developed several obligations on actors with respect to the downstream processing of data that would not ordinarily have a contractual underpinning. For example, a data provider is obliged to take reasonable and appropriate steps (including technical safeguards) to ensure that the recipient, as well any parties to whom the recipient may provide the data, complies with all the duties and restrictions that the data provider itself had to comply with for the benefit of a protected third party.[60]

## C. Reflections for the Commission

40. As noted by the Secretariat in its note on legal issues related to the digital economy (A/CN.9/1012, para. 25), despite their contractual underpinning, uncertainty exists as to the rights and obligations of the parties to data transactions. It is therefore proposed as part of the workplan put forward in that note that preparatory work should be undertaken by the Secretariat towards a legislative text on the rights and obligations of parties to data transactions for commercial purposes.

41. The creation of new rights in data as a commodity raises significant public policy issues by introducing a new legal regime for data that requires a careful consideration of the interests of actors involved and broader social, economic and legal impacts. In keeping with the emphasis of the Commission on "proposing

Individuals with regard to Automatic Processing of Personal Data, concluded under the auspices of the Council of Europe: United Nations, *Treaty Series*, vol. 1496, No. 25702.

[57] Ibid.

[58] ALI/ELI Principles, Preliminary Draft No. 3 (15 October 2019), on file with the Secretariat.

[59] ALI/ELI Principles, ALI Council Draft No. 1, principles 17–22.

[60] ALI/ELI Principles, Preliminary Draft No. 3, principle 27.

solutions that address legal obstacles and take into account public policy considerations",[61] it is not proposed that preparatory work on rights in data as a commodity should be undertaken at this time, but rather that exploratory work should continue in this area.

# V. Preliminary appraisal of relevant UNCITRAL texts

## A. CISG

### 1. "Sale" of "goods"

42. There has been a lively debate in the past couple of decades as to whether the United Nations Convention on Contracts for the International Sale of Goods (CISG) applies to software. The CISG applies to "contracts of sale of goods" (article 1(1)), and the debate has focused on two issues: first, whether software can be characterized as "goods" (a term that is not defined in the CISG), and second, whether the transfer of software under contract can be characterized as a "contract of sale".

43. On the first issue, the Secretariat observed in 2001 that the CISG "seems to embody a rather conservative concept of "goods", as it is considered both in legal writings and case law to apply basically to moveable tangible goods".[62] Thus, a disk or other physical medium incorporating computer code was "goods", but computer code acquired itself (e.g., by internet download) was not.

44. On the second issue, the Secretariat has previously observed that, while the term "contract of sale" is not defined in the CISG, its meaning can be determined by reference to its context, specifically the rights and obligations of the parties to the contract of sale provided under the CISG. Thus, the contract of sale involves the delivery of goods and transfer of property, and can thus be distinguished from a licence agreement.[63] Given that the supply of software involves the copying of data (i.e., the computer code) and does not involve the "transfer" of data, the supply can only be characterized as a licence and not a "sale". Conversely, in a 2015 decision, a district court of the Netherlands found that a software licence agreement was a "sale" for the purposes of the CISG in view of the fact that the use of the software was not limited in time and that it was transferred as the result of a single payment as opposed to monthly instalments.[64]

45. Turning from software to data transactions, an additional difficulty is presented in that, as noted above (para. 22), most legal systems appear not to regard data as "property". Nevertheless, the decision of the Court of Justice of the European Union in the case of *UsedSoft GmbH v. Oracle International Corp.*,[65] which concerned a different legislative context, might be used to liken some data transactions, particularly data provision contracts, to contracts of sale. For data-related service contracts, an additional question arises as to whether the provision of the service constitutes the "preponderant part" of the contract, thereby enlivening the exclusion in article 3(2) of the CISG.

### 2. Suitability of substantive provisions to data transactions

46. Even if the CISG were to apply to data transactions, a question arises as to whether its provisions are appropriate to address the needs of the parties. According to one commentary, the application of the substantive provisions of the CISG to data transactions does not pose any significant new problems, as most issues have already

[61] *Official Records of the General Assembly, Seventy-fourth Session, Supplement No. 17* (A/74/17), para. 210.
[62] A/CN.9/WG.IV/WP.91, para. 21.
[63] Ibid., paras. 27–28.
[64] Midden-Nederland District Court, *Corporate Web Solutions v. Dutch company and Vendorlink B.V.*, Case No. C/16/364668, Judgment, 25 March 2015.
[65] Case No. C-128/11, Judgment, 3 July 2012.

been discussed and litigated in the context of software transactions. Conversely, other commentaries caution against applying the CISG to new territories, which may have commercial reality different from "international sale of goods". While these comments were made with respect to software, they may be even more germane in the emerging field of data transactions.

47. An analysis of substantive provisions of the CISG reveals that the provisions discussed in the following paragraphs concerning rights and obligations of the parties may not be appropriate to address the needs of the parties to data transactions.

*Articles 38 and 39 – Time for examining goods*

48. Under article 38, the buyer is required to examine the goods, or cause them to be examined, within as short a period as is practicable in the circumstances. In data transactions, it is most likely that the buyer could examine transferred data only superficially and it does not have the means to check accuracy and completeness of the transferred data. Therefore, the time limits in article 39 for the buyer to give notice to the seller on a lack of conformity of the goods (i.e., within a reasonable time or two years at the latest) appear unreasonable in the context of data transactions.

*Articles 41 and 42 - Conformity of goods*

49. The application of articles 41 and 42 on the conformity of goods to data transactions raises a few questions. The use of data provided may be restricted by the application of the General Data Protection Regulation of the EU.[66] With regard to third party rights, issues relating to data ownership need to be taken into consideration. Furthermore, data transactions may be disrupted by the subsequent revocation of the consent to the use of the data by the concerned persons of personal data.

*Articles 45 and 74–77 – Damages*

50. The calculation of damages may be challenging in the area of data transactions; for example, the question of causality and the amount of damages, where data was acquired specifically for product marketing purposes and this is impaired due to the nonconformity of the data.

*Article 46 – Performance, substitute goods and remedy by repair*

51. If the goods do not conform with the contract, article 46 allows the buyer to require delivery of "substitute goods" under certain circumstances. Notably, the right for specific performance is not guaranteed and is restricted by the general rule in article 28, which provides that a court is not bound to enter a judgment for specific performance unless the court would do so under its own law in respect of similar contracts. Nevertheless, the requirement for delivery of "substitute goods" is likely to be unavailable in the context of data transactions, or inapplicable at all. In case of a damaged data carrier, which may be qualified as inadequate packaging according to article 35(2)(d), depending on the extent of the limitation of the use of the data, the repair of the data carrier or its substitution may be required.

*Article 52 – Early delivery, excess quantity*

52. In accordance with article 52, if the seller delivers the goods before the date fixed or delivers a quantity of goods greater than that provided for in the contract, the buyer may refuse to take delivery of all goods or of the excess quantity. In data transactions where the data is provided online (e.g., via email), it may not be possible for the buyer to refuse to take delivery, especially the excess portion of the data.

[66] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC.

*Article 55 – Open price contracts*

53. Where a contract has been validly concluded but does not expressly or implicitly fix or make provision for determining the price, the default rule in article 55 refers to the price generally charged at the time of the conclusion of the contract for such goods sold under comparable circumstances. The application of such default rule to data transactions may be challenging given the difficulty to determine "the price generally charged" in this context.

*Article 66 – Loss of the goods*

54. Article 66 deals with the passing of risk for loss of or damage to the goods. The buyer is still obliged to pay the price if loss of the goods happens after the risk has passed to the buyer, unless the loss is due to an act or omission of the seller. It is argued that the provisions on the transfer of risk (articles 66–70) can generally be applied to data and their optional character allows the parties to adapt the provisions to their needs. In data transactions, the concept of "loss" may relate to data security concerns but its meaning is not so easily understood. Arguably, even in case of an "assignment" of data, the seller will not erase a copy of the transferred data until the buyer has taken delivery and paid the price. In case of license of data, the seller will retain a copy of the transferred data and therefore such data will never be lost.

*Articles 85 and 86 – Preservation of goods*

55. Articles 85 and 86 set out the obligations of both parties to preserve the goods under certain circumstances. While the concept of "preservation of goods" makes sense in the context of tangible goods, it seems inapplicable to data. In practical terms, the quality of data may not change after a certain period of time and, therefore, the necessity to preserve data does not exist.

*Article 88 – Sale of goods*

56. Pursuant to article 88, a party who is bound to preserve the goods may sell them by any appropriate means if there has been an unreasonable delay by the other party in taking possession of the goods or in taking them back or in paying the price or the cost of preservation, provided that reasonable notice of the intention to sell has been given to the other party. This provision seems unsuited to data transactions because the contract may expressly limit the buyer's ability to transfer the data to a third party due to privacy or data security concerns.

## 3. Summary

57. Even if the CISG were to apply to data transactions, uncertainty as to how its substantive provisions would apply indicates that it is not an adequate solution for an international regime for the rights and obligations of parties to data transactions. Nevertheless, the CISG could serve as a model for developing a harmonized legislative solution in this respect.