Digital Trade in the Trade and Cooperation Agreement between the European Union, the European Atomic Energy Community and the United Kingdom of Great Britain and Northern Ireland

Dragoș Mihail MĂNESCU
Bucharest University of Economic Studies, Bucharest, Romania
dragos.manescu@drept.ase.ro

Abstract. In the context of the exponential growth in volume of digital trade and the diversification of its forms of implementation, the present article analyzed the framework provisions contained in the Trade and Cooperation Agreement between the European Union and the United Kingdom of Great Britain and Northern Ireland, provisions governing the conduct of post-Brexit digital trade.

Keywords: Digital Trade, Trade and Cooperation Agreement, Brexit, IT Services, direct marketing.

Introduction
After carrying out intense and difficult negotiations based on the provisions of art. 217 of the Treaty on the Functioning of the European Union, (which states that the Union may conclude agreements with one or more third countries or international organizations to create an association characterized by mutual rights and obligations, joint actions and special procedures) - ex Article 310 TEC – on 24.12.2020, just five days before the deadline of 01.01.2021 when the United Kingdom was to leave the largest trade alliance in the world, was concluded the Trade and cooperation agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (see text of the agreement: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:22020A1231(01)&from=RO).

The main document, namely the Trade Agreement, was supplemented by agreements on nuclear energy, agreements on the exchange of classified information and their protection, civilian nuclear energy and a number of joint declarations.

The trade agreement is essentially an economic and social partnership between the European Union and the United Kingdom. As the preamble to the agreement states, the parties wished, inter alia, to conclude an agreement between the United Kingdom and the Union in order to provide a legal basis for their future cooperation.

In this context, as we can speak of a real tabula rasa regarding the normative acts regulating the exit of a Member State from the European Union and, especially, regarding the future relations between the former partners from the perspective of their rights and obligations.

It should be noted that the previous experiences of Switzerland or EEA countries, such as Norway, in acquiring special status in relation to the European Union, are not directly transferable in the event of the United Kingdom's break with the European political bloc (Wall, 2020, p.289).

As a result, international treaties, agreements and other documents were used, such as the provisions of the Marrakesh Agreement (Wall, 2020, p.6) of 15 April 1994, which laid the foundations of the World Trade Organization or the Statute of the International Monetary Fund Agreement (regarding payments and transfers in respect of transactions carried out on the current
account of the balance of payments), as well as other instruments of multilateral and bilateral cooperation. Articles of Agreement (Statute) of the International Monetary Fund were adopted at the United Nations Monetary and Financial Conference (Bretton Woods, New Hampshire) on 22 July 1944. They were initially accepted by 29 countries and have since been signed and ratified by a total of 190 member countries.

**Provisions stipulated in the Title III of the Trade Agreement: Digital Trade.**

**Contextual analysis**

Title III of the Agreement addressed the regulatory issue of digital commerce in the context of the importance of facilitating new opportunities for businesses and consumers through digital commerce, while strongly counteracting unjustified barriers to data flows and e-commerce (preamble of the Agreement, p.6). All this with the simultaneous observance of the rules of personal data protection of the parties.

From the beginning, a clarification is needed. Digitalization, together with environmental protection and the fight against pollution, are the cornerstones of the European Union's future directions for sustainable economic development. A recent study (http://www.1asig.ro/Accenture-92-dintre-liderii-de-afaceri-considera-transformarea-digitala-o-prioritate-in-acest-an-articol-3,102-65470.htm): shows that 92% of the more than 6,200 business leaders and IT executives surveyed say that, for them, digital transformation is a priority in the near future.

Thus, it is not surprising that a large part of the funds for the financial recovery of EU economies will be directed, with priority, to these areas of development, namely digitization, environmental development and carbon footprint reduction (Next Generation EU Recovery Mechanism / EUR 672.5 billion Recovery and Resilience Mechanism over the next three years).

On the other hand, if we refer to digitization, it should be noted that it means much more than what is mentioned in Title III of the Agreement, namely digital trade. The concept of digitization covers areas from the digitization of agriculture, to the so-called European Digital Innovation Hubs/Centers, as part of the European Digitization Program. They aim at the widespread adoption of Artificial Intelligence, High Performance Computing (HPC) and cybersecurity, as well as other digital technologies, by the industry, in particular by Small and Medium/Midcaps (or mid-cap, refers to companies with a market capitalization or market value of between 2 and 10 billion dollars) and public sector organizations in Europe (https://ec.europa.eu/digital-single-market/en/european-digital-innovation-hubs-digital-europe-programme-0), in direct connection with the Digital Single Market Strategy for Europe (Proposal for a Regulation of the European Parliament and of the Council on questionable and fair markets in the digital sector (Digital Markets Law) /15.12.2020). Or, it is closely linked, for example, to the European Industrial Digitization Initiative, which refers to the so-called "fourth industrial revolution" (refers to technologies and concepts for organizing the value chain).

And all this in the light of the growing need for strict regulation of both digital commerce and the protection of the beneficiaries of this form of trading. Consumers of digital commerce need and demand from the authorities a maximum level of legal protection that must be manifested both through consumer protection legislation and private international laws due to the lack of identity and location of the parties, the dematerialized nature of electronic commerce and the risks associated with it (Gillies, 2008, p.2). This is all the more so as we observe a reversal of the historical trend according to which, in the past, laws on consumer protection and unfair competition
were drafted by public authorities more on their own initiative to achieve ethical and political goals, than following the need to respond to traders' requests (Hawk, 2016, p. 263).

There are opinions saying (Sharma, 2020, p. 412) that new technologies or technology-based services (including digital commerce) should come with public disclosures about how they work and how they use data, similar to the requirements of the Federal Drug Administration in United States and similar national bodies around the world in their area of competence.

At the same time, it must be taken into account that the commercial advertising, respectively the direct marketing referred to in art. DIGIT.14 and accompanying digital commerce erode confidentiality for financial gain, and spam has become a real waste/impediment from economic point of view, to virtually all businesses, and has generated specific legislation and special international agreements (Davidson, 2009, p.4). This while digital campaigns on social platforms can change history. And we only mention a few situations where there are solid data and indications that this happened: the 2016 US presidential election, the elections in EU member states, Iran, Venezuela, Ukraine and the Brexit referendum suspected of being manipulated by Russian influence (Sharma, 2020, p. 377).

Last but not least, with regard to trade in services, especially financial services, which takes place almost exclusively digitally, and where the UK has been predominant, other views (Wall, 2020, p. 289) consider it to be a key area in which EU Member States will seek to restore balance to their advantage, and should therefore be targeted as a preferred area of regulation.

It should also be noted that it is easy to see that environmental protection and the fight against climate change are the leitmotif of the preamble to the above-mentioned Agreement, being mentioned countless times as immutable objectives. In contrast, the digital area, although a key feature of the EU's investment and support plan for funding programs, is not as well highlighted, with a rather succinct reference to it.

The United Kingdom has stood out over time as one of the most active promoters of the idea of a liberalized digital market at EU level. In this context, against the background of the exponential development of digital trade, especially in the conditions of changing economic and consumption behaviors due to the coronavirus pandemic, the discussion on tariffs, customs union and the single market in the context of Brexit, tends to take second place, requiring a wise regulation with a lot of vision of how digital markets work (Adam, 2020, p. 259).

However, it is true that the agreement contains references to the protection of personal data. The very title of Chapter II announces that it regulates data flows (hence trade, digital trading) and the protection of personal data (see also Davidson, 2009, p. 218).

Thus, during the specified period (Article FINPROV.10A of the Agreement), the transmission of personal data from the Union to the United Kingdom will not be considered a transfer to a third country as defined by Union law, under certain conditions, inter alia, if it applies the data protection law of the United Kingdom in force on 31 December 2020, as provided for and incorporated, respectively, into United Kingdom law by the European Union (Withdrawal) Act (2018 with the European Union (Withdrawal) Act of 2018) and amended with the articles on data protection, as amended by Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 87 [2019 Regulations on Data Protection, Privacy and Electronic Communications (amendments etc.) (exit from the EU) (the "applicable data protection regime"), and provided that the United Kingdom does not exercise the powers designated without the agreement of the Union in the Partnership Council (see Article INST.1 which provides for the Partnership Council, that is a body that aims to ensure the correct interpretation and application of the Agreement, as well as the supplementary agreements. The Partnership Council is co-chaired...
by a member of the European Commission and a representative of the UK government at ministerial level. The Partnership Council shall meet at the request of the Union or the United Kingdom and in any case at least once a year. In accordance with Article FINPROV.10A of the Agreement, the specified period shall begin on the date of entry into force of this Agreement and subject to paragraph 5 (which refers to the exercise by the United Kingdom of the powers designated without the agreement of the Union in the Partnership Council or the limitations resulting from the alignment with the relevant Union data protection legislation), conclude:

(a) the date on which the European Commission takes decisions on the adequacy of the level of protection provided by the United Kingdom pursuant to Article 36 (3) of Directive (EU) 2016/680 and Article 45 (3) of Regulation (EU) 2016/679 or

(b) four months from the date on which the specified period begins, which period shall be extended by a further two months, unless one of the parties objects, the date retained being the one that occurs first.

This is all the more so as, by the end of the fourth year following the entry into force of the Agreement, the Partnership Council has the power to take decisions to amend it or any supplementary agreement, provided, of course, that such changes may be necessary to correct errors, remedy omissions or other deficiencies (Article INST.1, paragraph 4, letter d).

We conclude that without these references, the UK would now become a third country in terms of the application of the GDPR (Article FINPROV.10A of the Agreement).

At the same time, the Agreement regularly contains clauses that allow modifications, adaptations, re-evaluations, which could introduce a character of unpredictability and lack of certainty or force of imposition of its provisions. We also mention here the provisions of Art. DIGIT. 6 par. 2 which sets a revaluation period of three years from the date of entry into force of this Agreement but at the same time gives the possibility to re-evaluate, practically, whenever necessary. Thus, a Party may, at any time, propose to the other Party that it review the list of restrictions on cross-border data flows and that such review should "be considered with understanding" (Article DIGIT.6 paragraph 2 of the Agreement).

We consider that the term “understanding” mentioned here, and which is found several times during the Agreement, leaves room for multiple interpretations and random in the normative process as well as in the application of the provisions of the agreement in the field regulated by this chapter, respectively cross-border data flow.

In this context, Art. DIGIT.6 par. 1 enshrines, in its first part, a principle that the parties to the agreement must not restrict these flows in any way and even facilitate trade in the so-called digital economy (Article DIGIT.6, paragraph 1 of the Agreement).

Subsequently, the same paragraph mentions, we consider, by way of example and not limitation, the ways in which these limitations could be achieved and which are prohibited from being applied, namely:

(a) by requiring the use of computer installations or network elements in the territory of the Party for processing, including by requiring the use of computer installations or network elements that are certified or approved in the territory of a Party;

(b) by requesting that the data be located in the territory of the Party for storage or processing;

(c) by prohibiting storage or processing in the territory of the other Party;

(d) by making the cross-border transfer of data conditional on the use of computer facilities or network elements in the territory of the Parties or location requirements in the territory of the Parties.
These provisions aim to eliminate any attempts by the signatories to the Agreement to oblige users of electronic communications services to use the facilities of one of the Parties, installations which would not otherwise be used normally. Or thus limit access to the market of one of the parties by establishing various disguised barriers. We can encounter here the concept of "network neutrality", a concept that has provoked over time many technical disputes that later became political and which can be translated into the following principle: the authorities will not allow a regulated public network to ban a certain use of the network, if such use does not harm the network (Rothchild, 2016, p. 421).

The following provisions also establish in this direction that electronic transmissions are considered a supply of a service and they will not be subject to customs duties (Article DIGIT.8 of the Agreement). These provisions must be corroborated with the provisions of art. SERVIN.1.2 lit. e that 'cross-border trade in services' means the provision of a service (article SERVIN.1.2. lit. o - For the United Kingdom, the term service means any service, regardless of the sector, except for services provided in the exercise of governmental authority):

I) from the territory of one Party to the territory of the other Party;
II) in the territory of one Party to a consumer of services of the other Party.

In this context, it should be noted that Article DIGIT.17 on IT services, determines which services are considered IT services and related services, whether or not they are provided through a network, including the Internet. The enumeration contained in par. 1 lit. a-e is, this time, a limiting one, the services facilitated by computer services and related services, other than those listed in this paragraph, not being considered to be computer services and related services per se.

At the same time, the agreement stipulates the conditions under which a service is provided online, respectively when it is provided by electronic means and does not require the simultaneous presence of the parties. This way of providing the service will exclude, according to the Agreement, both the need and the possibility of a prior authorization for its provision or any other form of endorsement, authorization, etc. what could be adopted in this regard.

It is thus intended to eliminate, once again, any possibility for the parties to introduce any barriers or restrictions that may arise in the way of such transactions. This is given that Europe has spent and continues to spend huge sums of money to improve communications and air, land or sea transport systems - and thus succeed in reducing the time and distance in the movement of goods and services - but at the same time, seems willing to maintain or at least tolerate artificial legal or structural barriers that are no less effective than distance and rugged terrain in disrupting trade in goods and services, especially financial services (Gkoutzinis, 2006, p.XV).

Instead, a series of services are enumerated (Article DIGIT.9, para. 2: Paragraph 1 shall not apply to telecommunications services, broadcasting services, gambling services, legal representation services or services provided by notaries or equivalent professions in so far as they involve direct participation) that may be subject to this form of prior authorization or restriction but provided that they involve both direct participation and specific participation in the exercise of public authority, namely telecommunications services, broadcasting services, gambling services, legal representation services or services provided by notaries or equivalent professions.

These services, together with a number of others listed in the Agreement, when they are the subject of contracts concluded by electronic means, are excluded from free contracting or may be subject to restrictions.

These, together with other restrictions that we will list below, we consider to be, in the end, restrictions or barriers that may arise in the way of free digital trade. At the same time, we consider that these limitations do not establish, as it would be believed, the principles of free trade of
e-commerce but rather are the germs of future restrictions and future dissensions that will arise between the parties or a future regulatory excess. We also consider that, although the established principles are those of freedom in carrying out activities, the establishment, often within rather vague limits, of exceptions is not such as to create the preconditions for this claimed freedom.

Thus, the Agreement establishes at art. DIGIT.10 the obligation for the parties not to restrict in any way the conclusion of contracts by electronic means except when they concern certain categories of services. Restrictions or barriers identified by the parties as possible to arise during the contracting process may be, first and foremost, of a legal nature, generated by the legal system as a whole, or of any other nature (but not listed), likely to induce, once again, randomness in the regulation and application of the provisions of the agreement. We consider that regulation also refers to the so-called structural barriers raised in the way of international economic activities and defined by some authors (Gkoutzinis, 2006, p. 54) as the natural result of the international economic and legal order and the conflict between transnational markets and the need for national/local control and regulation. By way of example, we mention:

- legal plurality resulting from the fact that international banks operate in several legal systems;
- the legal diversity derived from the fact that legal systems adopt different rules for similar issues.

A number of other possibilities for restrictions on e-commerce in general are also introduced by specifying restrictions that may be introduced on, for example, electronic authentication and reliable electronic services (art. DIGIT.11). Without specifying exactly which is the exact category of transactions, the Agreement provides in para. 3 that “a party may provide that, for a particular category of transactions, the method of electronic authentication or the trusted service be certified by an accredited authority in accordance with its own legislation or meet certain performance standards, which are objective, transparent and non-discriminatory and focus exclusively on the specific characteristics of the category of transactions concerned”.

Analyzing this provision, we conclude that it is too general and rather has the character of a way that will affect future situations. We can even say, extrapolating, that the established obligation approaches the definition of the condition as a modality, as it is found in the New Romanian Civil Code, respectively the obligation whose effectiveness or abolition depends on a future and uncertain event (article 1399).

Performance standards will depend, alternatively and not cumulatively, on the specifics of the category of transactions, on the definition of objective, transparent and non-discriminatory criteria to be found in their own legislation and, last but not least, on the interpretation of certification criteria by a nationally accredited authority. All this, we believe, creates a regulatory vacuum rather than a legislative clarification.

Beyond those mentioned, of course, the principle is that of the obligation for the parties to accept electronic authentication and reliable electronic services, in any of its specific technical forms.

In this context, the Parties specify that no provision of the Agreement shall prevent a Party from adopting or maintaining measures concerning the protection of personal data and privacy, including with regard to cross-border transfers of data, provided that:

- the right of the Party to provide instruments to allow transfers under conditions of general application for the protection of transferred data;
- provided that it informs the other Party of any measure referred to in the paragraph which it adopts or maintains (Article DIGIT.7, paragraph 2 and 3 of the Agreement).
These provisions must, however, be mandatory and permanently related to the above, namely to the provisions of the relevant legislation existing on 31 December 2020 in the countries parties to the Agreement (Article FINPROV.10A of the Agreement). Exceptions are found for the protection of personal data and cross-border data transfers, and when regulatory cooperation (see also Craig, Búrca, 2011, p. 384, Case C – 275/06 Promusicae v Telefónica de España OR [2008] ECR I – 271 on the transposition of property rights, data protection and privacy in EU legislation on electronic commerce, intellectual property and electronic communications) in digital commerce (Article DIGIT.16. paragraph 2) is regulated. We believe that the provisions on digital commerce must necessarily be related to the provisions of the European Code of Electronic Communications (DIRECTIVE (EU) 2018/1972), although only a few states have transposed its provisions into national law so far (Greece, Hungary and Finland have notified the European Commission of the transposition of EU Directive 2018/1972).

From the beginning of Title III, it is specified that the Agreement does not apply to audiovisual services (Directive (EU) 2018/1808 amending Directive 2010/13/EU), a provision that is also found in art. 7 point 5 of the Decision adopted by the European Commission in Brussels on 27.12.2020.

Exceptions

The agreement provides for exceptions to the application of the rules on digital commerce (and not only) if the parties face situations that require action:

General Exceptions (Art. EXC.1)

The general exceptions are:

a) necessary for the protection of public security or public morality or for the maintenance of public order;

b) necessary to protect the life or health of humans, animals or plants;

c) necessary to ensure compliance with the laws, regulations or administrative provisions which are not contrary to the provisions of this Agreement (Article XX of the GATT 1994, including its Explanatory Notes and Additional Provisions, is incorporated into and forms an integral part of the Agreement and may be applied under certain conditions).

Before a Party adopts any of the measures set out in Article XX (i) and (j) of the GATT 1994 (https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm), that Party shall provide the other Party with all relevant information with a view to seeking a solution acceptable to the Parties. If no agreement is reached within 30 days of the provision of the information, the party concerned may apply the relevant measures. If exceptional and critical circumstances requiring immediate action make it impossible to inform or examine in advance, the party intending to take action may immediately apply the precautionary measures necessary to deal with the situation. The Party concerned shall immediately inform the other Party thereof.

At the same time, we believe that the guidance provided by the United Nations, which has developed some general principles for business and human rights, should be taken into account. Thus, states must take measures to protect against any human rights violations by various actors in their regulatory area and, at the same time, they must create the conditions for companies operating in their area of competence to respect human rights (Kulesza et al., 2016, p.127).

Security exceptions (Art. EXC.4)

They are necessary for the protection of its essential security interests:
I) related to the production or trafficking of weapons, ammunition and war material, as well as to the production, trafficking and transactions with other products and materials, services and technologies and economic activities, carried out directly or indirectly, for the purpose of supplying a military unit;

II) related to fissile and fusible materials or to the materials from which they are obtained;

III) in time of war or in other emergency situations within international relations;

IV) necessary for the fulfillment of its obligations under the Charter of the United Nations for the maintenance of international peace and security.

At the same time, the European Commission is concerned that Member States increase their readiness and improve cooperation between them, including by requiring critical infrastructure operators such as energy, transport and key information society service providers (e-commerce platforms, social networks, etc.) and public administrations to take the measures they deem necessary for the management of security risks and the reporting of serious incidents to the competent national authorities (Kulesza et al., 2016, p. 20).

Prudential exception (Art. SERVIN.5.39)

They are for:

a) the protection of investors, depositors, policyholders or persons to whom financial service providers have fiduciary obligations;

b) ensuring the integrity and stability of a party's financial system.

It should be noted that, unlike the General and Security Exceptions situation, in the case of Prudential Exceptions, if such measures are not compatible with the provisions of this Agreement, they may not be used by a Party as a means of evading to its commitments or obligations under this Agreement.

If they are part of a certification procedure, these exceptions also apply to the transfer of the source code of the software owned by a natural or legal person of the other party and access to it. Otherwise, the principle is, of course, that one party does not provide for the transfer of the source code belonging to an entity of the other party. The term "does not provide" should be construed here as "may not require" or "does not bind". Instead, the actors belonging to the parties, whether natural or legal persons, are free to transfer their source code or access to it at will (Article DIGIT.12 paragraph 2 of the Agreement).

The Agreement also establishes the principle that judicial authorities, those that have authority in the competition field, judicial or intellectual property protection authorities, as well as the competent public procurement agreement (GPA) (http://dce.gov.ro/poli-com/omc/17.pdf) authorities, are exempted from the above principle; and they may act, restrict or restrict the transfer or access to the source code, regardless of the party to whom it belongs or the form of organization of the owner. The Government Procurement Agreement (GPA) is one of the plurilateral agreements included in Annex 4 of the Agreement on the Establishment of the World Trade Organization (WTO). To date, 18 parties representing 46 WTO members have acceded to this Agreement. The European Union is a signatory to the GPA, the rights and obligations arising from this Agreement automatically applying to Romania from the date of accession to the European Union, January 1, 2007. The GPA establishes the legal framework of the rights and obligations of the Parties regarding legislation, procedures and good practices used in the field of public procurement, as well as how to resolve appeals. Its annexes provide, for each Member separately, including Romania, the governmental entities authorized to carry out these operations, as well as the categories of goods, services and construction works that fall under the scope of the
Agreement. Regarding the Government Procurement Agreement (GPA), we specify that, in addition to regulating the rights and obligations of the parties, the instructions, good practices and procedures for resolving disputes, it also includes standards on the use of electronic means (electronic commerce) in public procurement (Țurcan, Ungureanu, 2020, p. 27).

The agreement we are referring to sets out in Article DIGIT.13 a set of principles that must underpin the measures that states can take to protect consumer confidence in the online environment.

This is all the more so as we live in the age of the Internet and digitalization, Artificial Intelligence and NLP, in which business practices are increasingly using software known as electronic agents in digital commerce transactions. Thus, a computer program or electronic device or other automated means are used to initiate an action or to respond to electronic messages without even being supervised by a person. In a legal context, an electronic agent can be automated to allow contracts to be concluded or executed, as is the case, for example, when we purchase books, CDs, airline tickets and other goods and services from a website such as Amazon.com (Mallor et al., 2013, p. 936).

Against this background, we consider that the provisions of art. DIGIT.14 para. 1 and 2 according to which each party shall ensure that users are effectively protected against unsolicited direct marketing communications and shall ensure that direct marketing communications are not sent to users who are individuals, unless they have given their consent, also aim to protect trust in digital commerce and protect consumers of online services. And also the provisions of art. DIGIT.15 on open public data which recognizes that facilitating public access to public data and the use of public data contributes to stimulating economic and social development, competitiveness, productivity and innovation. We can even consider that this paragraph 1 of art. DIGIT.15 is rather a statement of principles that should guide all international trade.

At the same time, facilitating access to public data is in opposition to growing consumer concerns about intimacy and protection of privacy, especially as simple online searches can turn into real harassment with offers and unsolicited direct marketing communications.

**Conclusion**

What we consider important to note is that the principles set out in art. DIGIT.13 para. 1 lit. a-d should not, at any time, become a means of blocking digital trade relations between the signatory states of the agreement or of disguised barriers to data flows. This is because par. 2 recognizes the importance of national consumer protection agencies or institutions with such responsibilities in order to protect their consumers (we consider that the mandate and limits of the competence of the Body of European Regulators for Electronic Communications (BEREC) should also be taken into account), as well as to increase their confidence in digital commerce, and also recognizes the importance of cooperation between them. The cooperation is also enacted within art. DIGIT.16 which provides that the Parties shall exchange information on regulatory matters in the context of digital commerce, except in those situations, incidental to the protection of personal data and privacy, including, also, cases of cross-border transfers of personal data.

However, no concrete guarantees, limitations or modalities of action regarding possible abuses of power by these institutions or bodies are presented, nor are there any tangible ways in which those affected, consumers or other parties involved other than consumers per se may act as such, as it happens in the article DIGIT.14, par. 5 regarding remedial measures against senders of direct marketing communications that do not comply with the limits set by the competent authorities of the countries party to the Agreement.
Accordingly, we are of the opinion that the provisions of the above-mentioned Articles should be corroborated with the provisions of Chapter 4 of the Agreement: Technical Barriers to Trade and Art. DIGIT.16: Regulatory Cooperation on Digital Trade and Art. COMPROV.11: Global cooperation on issues of common economic, social and environmental interest.

We consider that, also in the sense of eliminating the randomness or the lack of clarity, comes also par. 2 in art. DIGIT.15 which, after establishing the possibility, and not the obligation, for the parties to make public data available to the public, provides clear criteria that the data and the advertising process itself must meet. Moreover, if a party chooses to make public data available to the public, these criteria and conditions become mandatory and, at the same time, come with the obligation to update public data regularly. We see, therefore, that by virtue of the agreement, a clear obligation regarding public data and their publicity is not enacted, but once such a process of making such data public by one of the parties is initiated, it will assume a series of obligations strictly provided by law (Article DIGIT.15 paragraph 2, lit. a-g).

Last but not least, in par. 3 again calls for cooperation between the parties in order to identify ways in which each party can extend access to and use of the public data that the party has made public, in order to strengthen business opportunities and generate new ones, beyond the use of those data by the public sector. Basically, the aim is to give an economic and patrimonial dimension to this approach of making data public.

The analysis of this Title III leads us to consider that rather general guidelines are established to guide the activity in the regulated areas, without being able to give security or guarantees regarding its observance or the observance of the rights and obligations of its subjects, natural and legal persons, citizens of the European Union and the United Kingdom, respectively. Against this background, we find in the doctrine (Dickie, 2005, p. 130) the idea that the European Union, through regulations enacted over time, and from which this matter is no exception, has been rather moderately successful in providing a framework reflecting the diffuse and evolving nature of the notion of fair commercial interest of consumers, as well as ensuring a clear and concrete possibility of recovering the loss suffered in those cases where, for example, goods purchased electronically from a producer are not in accordance with the contract. Because, in the end, this is probably the key to building consumer confidence in cross-border e-commerce (Dickie, 2005, p. 130).

For specific details or issues, niche regulations will probably be used. This, we are sure, will lead, very quickly, to many divergences and to the need for further interpretations, clarifications and negotiations which will most likely take place in the Partnership Council, the Expert Groups, the Specialized Committees, up to the establishment of arbitral tribunals with members from the list established by the Agreement (article INST.27 List of arbitrators of the agreement).

Last but not least, if, throughout the history of the European Union, the Community, rather than individual Member States, has dominated the process of legislative enactment in the European e-commerce market (Dickie, 2005, p. 139), we can expect more and more initiatives from Member States to act as individual actors (see Poland and Hungary's positions on technology companies operating social media platforms: In January 2021, Poland proposed a set of laws that would create the conditions for large technology companies operating social media networks to be sanctioned then, when removing content that is not contrary to Polish law. Hungary has announced a similar initiative, given that the European Union wants a coordinated approach to the treatment of social media content: https://www.zf.ro/business-international/ungaria-o-ia-pe-caleza-poloniei-si-declara-razboi-marilor-companii-de-19899458) or call for collective action (See the initiative by France
and the Netherlands to create a European Union authority to regulate large technology companies such as Google and Facebook, which dominate the Internet: https://www.zf.ro/business-international/front-comun-impotriva-marilor-giganti-din-technologie-franta-si-19663789) in regulating gaps or in providing legislative incentives, or, on the contrary, discouraging means for digital behavior in general and digital commerce in particular.

References
Adam, R.G. (2020). Brexit Causes and Consequences, Ed. Springer Nature Switzerland AG.
Craig, P., de Búrca, G. (2011). EU Law. Text, Cases, and Materials (5th ed.), Oxford, Oxford University Press.
Davidson, A. (2009). The Law of Electronic Commerce, Cambridge University Press, Spam Act from 2003 and Memoranda of Understanding between Australia, South Korea and the USA.
Dickie, J. (2005). Producers and Consumers in EU E-Commerce Law, Oxford, Hart Publishing.
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.
Directive (EU) 2018/1808 amending Directive 2010/13 / EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Services Directive audiovisual media) given the evolution of market realities.
Gillies, L.E. (2008). Electronic Commerce And International Private Law, Cornwall, England, Ashgate Publishing Limited.
Gkoutzinis, A.A. (2006). Internet Banking and The Law in Europe Regulation, Financial Integration and Electronic Commerce, New York, Cambridge University Press.
Hawk, B., (2016). Law and Commerce in Pre-Industrial Societies, Leiden, The Netherlands, Koninklijke Brill NV.
Kulesza, J., Balleste, R., Horten, M. (2016). Cybersecurity and Human Rights in the Age of Cyberveillance, London, Rowman & Littlefield.
Mallor, J.P., Barnes, A.J., Bowers, T., Langvardt, A.W. (2013). Business Law. The Ethical, Global, and E-Commerce Environment, (15th ed.), New York, Ed. McGraw-Hill/Irwin.
Proposal for a Regulation of the European Parliament and of the Council on questionable and fair markets in the digital sector (Digital Markets Law) /15.12.2020
Rothchild, J.A. (2016). Research Handbook on Electronic Commerce Law, Cheltenham, UK, Edward Elgar Publishing Limited.
Sharma, S. (2020). Data Privacy and GDPR Handbook, Hoboken, New Jersey, Ed. John Wiley & Sons, Inc.
The Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, Preamble, p. 8.
Țurcan, V., Ungureanu, C. (2020). Mapping the commitments assumed by the Republic of Moldova within the international agreements regarding sustainable public procurement, Institute for Development and Social Initiatives “Viitorul”.
Wall, S. (2020). Reluctant European. Britain and the European Union from 1945 to Brexit, Ed. Oxford University Press.
https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:22020A1231(01)&from=RO
http://www.1asig.ro/Accenture-92-dintre-liderii-de-afaceri-considera-transformarea-digitala-o-prioritate-in-acest-an-articol-3,102-65470.htm: According to the report Accenture (NYSE:
ACN) Technology Vision 2021 entitled " Leaders Wanted: Masters of Change at a Moment of Truth," based on a study conducted in early 2021.

https://ec.europa.eu/digital-single-market/en/european-digital-innovation-hubs-digital-europe-programme-0.
https://ec.europa.eu/digital-single-market/en/fourth-industrial-revolution.
https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm.
http://dce.gov.ro/poli-com/omc/17.pdf.
https://www.zf.ro/business-international/ungaria-o-ia-pe-calea-poloniei-si-declara-razboi-marilor-companii-de-19899458.
https://www.zf.ro/business-international/front-comun-impotriva-marilor-giganti-din-tehnologie-franta-si-19663789.