ANALELE ŞTIINŢIFICE
ALE
UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
(SERIE NOUĂ)

ŞTIINŢE JURIDICE

TOM LXVII / supliment 2, 2021

Editura Universităţii „Alexandru Ioan Cuza” din Iaşi

ISSN: 1221-8464
ISSN-L: 1221-8464

Adresa redacţiei:
Universitatea „Alexandru Ioan Cuza" din Iaşi
Facultatea de Drept
Bd. Carol I, nr. 11
Iaşi, România, 700506

Volumul are la bază lucrările conferinţei internaţionale
Perspective juridice asupra Internetului *– ediția a V-a –*
Spațiul virtual, ultima frontieră? Încheierea și executarea contractelor,
care s-a desfăşurat pe 30 octombrie 2021, online,
la Universitatea „Alexandru Ioan Cuza" din Iaşi, Facultatea de Drept.

Proceedings of the international conference
Legal Perspectives on the Internet *– 5th Edition –*
Cyberspace, the Final Frontier? Concluding and Performing Agreements,
which took place online on October 30th 2021
at "Alexandru Ioan Cuza" University of Iași, Faculty of Law.

Cuprins

TEHNOLOGII DISRUPTIVE ÎN DREPTUL PRIVAT

DREPTUL PUBLIC ÎN ERA DIGITALĂ

Table of contents

DISRUPTIVE TECHNOLOGIES IN PRIVATE LAW

PUBLIC LAW IN THE DIGITAL ERA

TEHNOLOGII DISRUPTIVE ÎN DREPTUL PRIVAT

DISRUPTIVE TECHNOLOGIES IN PRIVATE LAW

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-1

Cyberspace, the Final Frontier? Concluding and Performing Agreements. Unfair Terms in B2B Adhesion Contracts

Cyberspace, ultima frontieră? Încheierea şi executarea contractelor. Clauze abuzive în contractele de adeziune B2B

Carmen Tamara Ungureanu[1]

Abstract: If a few years ago the virtual space was a „place” considered exotic for concluding contracts, now it is a common practice. The vast majority of contracts can be concluded online and most of them are adhesion contracts. Adhesion contracts (take-it-or-leave-it) are a consequence of trade modernization and are absolutely necessary. Nevertheless, they carry their own special risks, no matter the adherent's quality, that of a consumer or a professional. One of the risks is that of acceptance by the adherent of unfair terms imposed by the other contractual party. We will not discuss the unfair terms in consumer contracts, but those embedded in B2B contracts. Starting from the relatively recent legislative changes in European law and the laws of certain member states (Germany and France in particular) we will show that the current trend is to sanction abusive clauses/unfair terms in adhesion contracts, irrespective of the contract type, B2C or B2B.
Keywords: adhesion contracts; B2B contracts; unfair terms

Rezumat: Dacă în urmă cu câţiva ani spaţiul virtual era un „loc” considerat exotic pentru încheierea contractelor, în prezent este o practică obişnuită. Marea majoritate a contractelor se pot încheia online şi cele mai multe dintre ele sunt contracte de adeziune.Contractele de adeziune (*take-it-or-leave-it*) reprezintă o consecinţă a modernizării comerţului şi sunt absolut necesare. Acestea ascund, însă, riscuri, indiferent de calitatea aderenţilor, consumatori sau profesionişti. Unul dintre riscuri este acela al acceptării de către aderent a clauzelor abuzive, impuse de cealaltă parte contractantă. Nu vom discuta despre clauzele abuzive din contractele cu consumatorii, ci despre cele încorporate în contractele B2B. Pornind de la modificările legislative relativ recente din legislaţia europeană şi din aceea a anumitor state membre (Germania şi Franţa în special) vom arăta că tendinţa actuală este de a sancţiona clauzele abuzive din contractele de adeziune, indiferent de tipul contractelor, B2C sau B2B.
Cuvinte-cheie: contracte de adeziune; contracte B2B; clauze abuzive

[1] Professor PhD, Faculty of Law, “Alexandru Ioan Cuza” University of Iași, e-mail: carmen.ungureanu@uaic.ro.

Introduction

If a few years ago the virtual space was a "place" considered exotic for concluding contracts, now it is a common practice. The vast majority of contracts can be concluded online and most of them are adhesion contracts.

Adhesion contracts or, in other words, *standard form contracts*[2], are a consequence of trade modernization. "[C]ontracts of adhesion are a welfare-enhancing feature of modern commercial life. For firms, the very uniformity and rigidity of such contracts makes them valuable as a means of reducing agency costs and fixing expectations of future obligations. For consumers, not having to bargain is valuable as well"[3]. Imagine what it would mean to negotiate each contract for buying goods at a supermarket, for public transportation, for online services, for creating an email address or an account on a platform, etc. "The costs of reading, understanding, and bargaining over every term in such contracts would be enormous"[4].

Due to the frequency of consumer contracts, there is a misconception that the only adhesion contracts would be the B2C contracts. The truth is that almost any type of contract can be an adhesion one. Thus, adhesion contracts can be contracts concluded by consumers with professionals (consumer contracts or B2C – business-to-consumers), individual employment contracts, insurance contracts, contracts concluded between professionals (B2B – business-to-business), etc. An extreme type of adhesion contract is the so-called *smart contract*, whose applicability has taken a momentum in the framework of the growing blockchain technology and DLT (*distributed ledger technology*)[5].

Not all contracts that can be concluded and performed in the virtual space will be analyzed here, not even all of the adhesion contracts, but only one of the

[2] J. Gordley, *In defense of Roman contract law*, in P. G. Monateri (ed.), *Comparative Contract Law*, Edward Elgar Publishing, 2017, ebook, p. 37.

[3] A. Tutt, *On the Invalidation of Terms in Contracts of Adhesion*, Yale Journal on Regulation, vol. 30, no. 2/2013, p. 442, [Online] at http://digitalcommons.law.yale.edu/yjreg/ vol30/iss2/5, accessed 10.08.2021.

[4] *Ibidem.*

[5] This type of contract will not be discussed in this paper. For the analysis of smart contracts in the legal literature, see, M. Durovic, F. Lech, *The Enforceability of Smart Contracts*, The Italian Law Journal, vol. 5, no. 2/2019, p. 493 et seq., https://doi.org/ 10.23815/2421-2156.ITALJ, [Online] at https://www.theitalianlaw journal.it/duroviclech/, accessed 11.11.2021; J. Bacon, J.D. Michels, C. Millard, J. Singh, *Blockchain Demystified*, Queen Mary School of Law Legal Studies Research Paper No. 268/2017, p. 27, [Oline] at https://ssrn.com/abstract=3091218, accessed 11.11.2021; G. Rühl, *Smart (legal) contracts, or: Which (contract) law for smart contracts?*, March 10, 2020, in B. Cappiello, G. Carullo (eds.), *Blockchain, Law and Governance*, Springer, p. 2, [Online] at https://ssrn.com/abstract= 3552004, accessed 11.11.2021.

risks to which the parties in the adhesion contracts are exposed to will be singled out, namely that of accepting *unfair terms* or, in other words, *abusive clauses*[6].

In this endeavor, the meaning of 'adhesion contract' (1) and that of 'unfair terms' (2) will be first clarified. The need for protection of professional adherents will then be explained (3) and European and national approaches to unfair terms between professionals (4) will be addressed, concluding that the current trend is to protect adherents, regardless of their quality, of consumers or professionals.

1. The meaning of 'adhesion contract'[7]

In European law the concept of adhesion contract is not defined, but it is nevertheless used (for example, in Article 3 of Directive 93/13/EEC on unfair terms in consumer contracts[8]), and different types of contracts regulated in certain domains meet the characteristics of the adhesion contract, as it appears in some national legislations.

In the Romanian Civil Code, certain articles were dedicated to the adhesion contract[9], taking over a part of the regulation in this field of the Civil Code of Québec. The meaning of *adhesion contract* is set in article 1175 of the Romanian Civil Code, as the contract with the *essential* clauses imposed or drawn up by one of the parties, on his/her behalf or upon his/her instructions, which are not negotiable, the other party accepting them as they are[10].

Considering that the definition is similar to that in article 1379 of the Civil Code of Québec[11], its comments from the legal literature and the according legal practice will be taken into consideration. Thus, the characterization of a contract as being an adhesion one implies cumulatively meeting two elements: a) *the essential* clauses of the contract have to be *imposed* by one of the parties; b) the

[6] The notions of *unfair terms* and *abusive clauses* are going to be used interchangeably in this paper.

[7] C.T. Ungureanu, *The Romanian Adherent, Party to the Transnational Adhesion Contract,* in *Studies of Business Law - Recent Developments and Perspectives*, Peter Lang, Berlin, 2013, pp. 263-266.

[8] OJ L 95/29, 21.4.1993, with its subsequent amendments.

[9] The articles from the Civil Code in which there are referrals to the adhesion contracts are: article 1175, article 1269 (2), article 1671 and article 2515.

[10] In the legal literature, it was appreciated that, from the definition of the adhesion contract it can be noted that a contract can be qualified as being an adhesion one, either when the essential clauses were imposed by one of the parties or when they were drawn up by one of the parties; from the final part of the text it can be deduced that there is no adhesion contract unless the essential clauses are imposed to the adherent; see, for this, A.-A. Moise, *Sources of Obligations*, in *The New Civil Code. Comments on articles*, C. H. Beck Publishing House, Bucharest, 2012, p. 1229.

[11] Article 1379 Civil Code of Québec: « Le contrat est d'adhésion lorsque les stipulations essentielles qu'il comporte ont été imposées par l'une des parties ou rédigées par elle, pour son compte ou suivant ses instructions, et qu'elles ne pouvaient être librement discutées. », [Online] at http://legisquebec.gouv.qc.ca/en/showversion/cs/CCQ-1991?code=se:1379 &pointInTime =20170915, accessed 09.11.2021.

other party has to find itself in the *impossibility of negotiating* the contract. It was stated that the nature of the contract or the quality of the parties is not relevant[12]. The imbalance between the contractual parties regarding their economic, legal or informational power does not justify *in abstracto* considering a contract as an adhesion one; it has to be established if one of the parties was in the impossibility to negotiate the clauses of the contract[13]. It is not sufficient that a contract be drawn up by one of the parties or for her/him by a third party (for example, a lawyer), but it has to be *imposed* to the other party, to the adherent.

As a consequence, the adherent is *always* in a position of inferiority towards the stipulant, no matter what his/her quality is, a professional or a contractual party considered vulnerable, in need for protection.

As to the *essential character* of the contractual clauses, this has to be examined in each particular case, by the court; what is not essential to one contractual party, could be essential to the other one. In the Québec case law, the courts set up in different situations the meaning of 'essential clauses'. For instance, in an intellectual property contract four clauses were considered to be essential: the exclusivity clause, the penalty clause, the amount of money which the artist should receive and the contract period[14].

The clauses of the adhesion contract are, as a rule, standard clauses (*boilerplate clauses*) defined in art. 1202 (2) of the Romanian Civil Code as stipulations previously established by one of the parties to be used generally and repeatedly and which are included in the contract without having been negotiated with the other party. It is possible, however, that the adhesion contract also includes clauses that are not „generally and repeatedly" used by the stipulant, but are imposed on certain adherents. The standard clauses, if they fall into any of the types listed in art. 1203 of the Romanian Civil Code are considered *unusual clauses* or, in other words, *surprising terms*, which do not produce effects unless they are expressly accepted in writing by the other party[15].

The terms of the adhesion contract, whether standard or not, could be unfair terms with a content that disadvantages or even harms the adherent.

2. The meaning of 'unfair terms' in an adhesion contract

Adhesion contracts hide inside the risk for adherents to accept unfair terms, either because they express their consent without knowing the contractual clauses (often the adherent signs the contract or, to be accurate, ticks an icon without

[12] B. Lefebvre, *Le contrat d'adhésion*, in "La Revue du Notariat", Montréal vol. 105, september 2003, p. 444, https://doi.org/10.7202/1045922ar, [Online] at https:// papyrus. bib.umontreal.ca/jspui/bitstream/1866/1386/1/Contrat%20d'adhesion.pdf, accessed 18.11.2021.

[13] B. Lefebvre, *op.cit*, p. 446.

[14] *Rousse* c. *Dion*, J.E. 2001-1213 (C.Q.) as cited by B. Lefebvre, *op. cit.*, p. 447, note 24; R. Baudouin, *Code civil du Québec annoté*, tome II, 14th Edition, Wilson & Lafleur Itée, 2011, p. 1649 et seq.

[15] For an analysis of unusual clauses, see, I.-F. Popa, *„Tirania" clauzelor neuzuale*, Revista Română de Drept Privat, no. 1/2016.

reading the contract), or because, although they know the contract terms, accepts them anyway, being constrained by the need to conclude the contract[16].

In most cases only two people read the terms of the adhesion contract: the lawyer who drafted the clauses, which are frequently taken from different sources of standard clauses/boilerplate clauses, and he/she may not go through either carefully and include them in the contract because they are part of the common practice in a particular field[17] and the second person reading them is the adherent's lawyer, who explains to his client what he/she has undertaken through the contract and that there are great chances to not recover the damage suffered.

The notion of an unfair contractual term is defined in the European consumer protection law, in article 3 of Directive 93/13/EEC on unfair terms in consumer contracts, as a contractual term which has not been individually negotiated, if, „*contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer*". A contractual term should „*always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract*".

The Directive has been transposed into the legislations of the Member States so that consumers are protected from unfair contract terms, in particular those of adhesion (standard contracts). In Romanian law, the unfair term in contracts concluded between consumers and professionals[18] is the clause that has not been negotiated directly with the consumer and that creates, by itself or together with other provisions of the contract, a significant imbalance between the rights and obligations of the parties, contrary to the requirements of good faith. The sanction of inserting an abusive clause in the contract is set by the court, on a case-by-case basis. The expression used by the legislator in the law[19], according to which abusive clauses *do not produce effects on the consumer*, and the contract continues to bind the parties if it can remain in force without the unfair terms, has been interpreted

[16] S. Guillemard, D. É. Onguene Onana, *Le contrat d'adhésion : actualités et droit international privé*, Les Cahiers de droit, Vol. 48, no. 4/2007, p. 646, https://doi.org/10.7202/043948aradresse copiée, [Online] at https://www.erudit.org/ fr/revues/cd1/2007-v48-n4-cd3850/043948ar/, accessed 2.11.2021; S. Guillemard, D.É. Onguene Onana, *op.cit*, p. 646.

[17] R. E. Scott, S. J. Choi, M. Gulati, *Revising Boilerplate: A Comparison of Private and Public Company Transactions*, Wisconsin Law Review, 2020, p. 629, [Online] at https://scholarship.law.duke.edu/faculty_scholarship/4038/, accessed 10.11.2021.

[18] Law no. 193/2000 on abusive clauses in contracts concluded between professionals and consumers, republished in Official Gazette (hereinafter O.G.) no. 543, 03.08.2012.

[19] Article 6 from Law no. 193/2000.

in the legal literature in the sense that the applicable sanction[20] is *absolute partial nullity*[21].

In the EU law and in the national law of the Member States, as a result of the implementation of European directives, the annulment/ineffectiveness of unfair terms is therefore reserved for consumers[22]. The adherents who are not consumers usually do not enjoy any special protection with regard to unfair terms.

However, the issue of unfair terms in B2B (business-to-business) contracts has been a concern for the European legislator, who in 2011 discussed an instrument developed by the European Commission Expert Group on European Contract Law, which contained proposals on this matter[23]. Article 85 of the instrument provided that „in contracts between businesses a non-individually-negotiated term is unfair only if it significantly disadvantages the other party and is of such a nature that its use grossly deviates from good commercial practice, contrary to good faith and fair dealing." [24]. In this way, the Expert Group treated the unfair terms in B2B contracts differently, compared to those in consumer contracts (as defined above).

The contractual unfair term in this meaning was included in the proposal for a Regulation on a Common European Sales Law[25], in Article 86. However, the

[20] In legislation, in order to indicate the sanction of ineffectiveness of a clause inserted in a contract, invalidly concluded, expressions such as the following can be used: "the clause is deemed unwritten", "the clause is without effect", "the clause is inoperative" and, less often, "the clause is null". All these expressions used in the Romanian legislation were taken from the EU legislation (where, given the diversity of existing sanctions in the Member States, neutral terms were used; an illustrative example is the *sanction of non-effect of the abusive clauses* of Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (see, S. Gaudemet, *La clause réputée non écrite*, Editions Economica, Paris, 2006, pp. 75-76). The definition of these sanctions and the distinction among them are not covered by this paper.

[21] L. Pop, *Tratat de drept civil. Obligațiile. Vol. II. Contractul*, Universul Juridic Publishing House, Bucharest, 2009, pp. 333-335.

[22] Legal literature abounds in articles and books on this topic, among them: L. Bercea, *Acţiunile colective în eliminarea clauzelor abuzive din contractele standard de consum. Cui prodest?,* in Revista Română de Drept Privat, no. 3/2013, pp. 24-36; J. Goicovici, *Dreptul consumaţiei*, Sfera Juridică, Cluj-Napoca, 2006.

[23] M.W. Hesselink, *Unfair Terms in Contracts Between Businesses*, in J. Stuyck, R. Schulze (eds.), *Towards a European Contract Law,* Sellier European Law Publishers, 2011, pp. 131-148.

[24] M.W. Hesselink, *op. cit.*, p. 132.

[25] Bruxelles, 11.10.2011 COM (2011) 635 final 2011/0284 (COD), [Online] at https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52011PC0635&from=EN, accessed 08.08.2021.

proposal was withdrawn in 2014[26] on the grounds of a new proposal to include e-commerce in the digital single market[27].

Unfair contractual terms in B2B contracts is an issue discussed in the Anglo-Saxon law system, as well. In American law, certain clauses within an adhesion contract could be unenforceable/deemed „unconscionable" by applying the unconscionability doctrine[28]. „In contract law, a contract is defined unconscionable when it is unfair or extremely one-sided in favor of the party who has the superior bargaining power. An unconscionable contract can be defined as an agreement that mentally competent people would not enter into and that no fair and honest person would accept"[29].

3. Why would adherents-professionals need protection?

People in a state of vulnerability need protection. In adhesion contracts adherents are vulnerable, as they are made for various reasons to accept the clauses imposed by the stipulant, elaborated in his/her favor. Legislative protection would result in contract rebalancing, with the contracting parties returning to a certain position of equality[30].

In any contract one of the parties imposes himself/herself on the other, because there cannot be a perfect balance between the economic, legal, informational, bargaining power of the parties. All the more so in the case of adhesion contracts, the freedom of contract principle suffers, as the adherent has only the freedom to choose between contracting (under the conditions imposed by the other party) and not contracting.

---

[26] Commission Work Programme 2015, A New Start, Strasbourg, 16.12.2014, COM (2014) 910 final. Annex II: List of withdrawals or modifications of pending proposals, item 60, [Online] at https://ec.europa.eu/info/sites/default/files/cwp_2015_annex_ii_en.pdf, accessed 09.08.2021.

[27] For explanations on the failure of the proposal, K. Norris, *Common European Sales Law: A Missed Opportunity or Better Things to Come*, in Business Law Review, vol. 37, no. 1/2016, pp. 29-32; M. Király, *The Rise and Fall of Common European Sales Law*, in Elte Law Journal, no. 2/2015, pp. 31-42, [Online] at https://eltelawjournal.hu/rise-fall-common-european-sales-law/, accessed 08.08.2021.

[28] We will not analyze the American approach here. For a presentation of the doctrine of unconscionability, see C.A. Rodriguez-Yong, *The Doctrines Of Unconscionability And Abusive Clauses: a Common Point Between Civil And Common Law Legal Traditions*, Oxford University Comparative Law Forum, 2011, [Online] at https://ouclf.law.ox.ac.uk/the-doctrines-of-unconscionability-and-abusive-clauses-a-common-point-between-civil-and-common-law-legal-traditions/, accessed 12.08.2021; E. D'Agostino, *Contracts of Adhesion Between Law and Economics. Rethinking the Unconscionability Doctrine*, Springer, 2015, ebook; N. Browne, L. Biksacky, *Unconscionability and the Contingent Assumptions of Contract Theory*, Michigan State Law Review, 2013, pp. 212-255, [Online] at https://scholarworks.bgsu.edu/ econ_pub/11/, accessed 12.08.2021.

[29] E. D'Agostino, *op. cit.*, p. 7.

[30] M.W. Hesselink, *op. cit.*, pp. 132-134.

There are many asymmetries between professionals who enter into contracts, related to various factors, such as: complexity of goods or services which contracting on, experience in contracting and negotiation, understanding the meaning of legal or economic terms, the economic dependence of one professional on the other, etc. For example, imbalances occur in the relationship between a trader and a distributor, between a franchisor and a franchisee, between farmers in distribution chains, and so on. In these cases there is mainly a matter of economic dependence. Contracts characterized by economic dependence are those in which one of the professionals, the adherent, is dependent on a regular, privileged or exclusive relationship with his contractual partner, which has the effect of placing him in a state of dependence and domination, in exchange for his survival on the market[31].

The professionals, as adherents, are in a state of vulnerability similar to that of consumers. Besides that, in an adhesion contract the adherent is vulnerable, whether he is a consumer or a professional, by the simple fact that he cannot influence the content of the contractual clauses, which are pre-written by the stipulant in his/her favor.

Does a person need protection in this capacity as adherent or does it have to take all the necessary measures and bear the risks of the economic activity in which it has engaged? But if he is economically dependent on the stipulant, does that mean he has a choice between entering into the contract and going bankrupt? If the idea of applying the *caveat emptor* principle were accepted, without any exception, then implicitly the abuse of power of the professionals as stipulants would be justified and an unfair competition would be considered as representing normality.

The rules on commercial competition are not sufficient to ensure the use of fair trade practices. The objectives of commercial competition law, moreover, are to guarantee fair competition in the market and not to protect the interests of individual competitors[32]. Therefore, legislative intervention in this area seems to be necessary, aiming at restricting the use of unfair terms, ensuring a market characterized by fair competition and economic stability. Abusive clauses can threaten the entire economic system. For example, if the stipulant imposes jurisdiction clauses in favor of a state court or arbitral tribunal, which are

[31] G. Virassamy, *Les contrats de dépendance, essai sur les activités professionnelles exercées dans une dépendance économique*, Librairie Générale de Droit et de Jurisprudence, Paris, 1986, p. 10.

[32] I. Graef, *Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence*, in Yearbook of European Law, Vol. 38, no. 1/2019, p. 450, https://doi.org/10.1093/yel/yez008, [Online] at https://research.tilburguniversity.edu/en/publications/differentiated-treatment-in-platform-to-business-relations-eu-com, accessed 04.08.2021.

prohibitive for the adherent, in terms of distance, language, costs, this may ultimately lead to the adherent's exit from the market, being unable to recover[33].

4. European and national approaches to unfair terms between professionals[34]

Both in European law (sectoral only) and in the legislation of certain EU Member States, including Germany, France, Belgium[35], the Netherlands, there have been some relatively recent legislative changes[36], by which unfair terms in contracts are sanctioned regardless of the type of contract in which they were embedded, thus applying not only to consumer contracts, but also to B2B contracts.

At the European level, Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services[37], known as the P2B (*platform-to-business*) Regulation, has been adopted. This Regulation recognizes that online platforms enter into contracts with companies using their services (especially micro, small and medium-sized enterprises) from a position of superiority „*which enables them to, in effect, behave unilaterally in a way that can be unfair and that can be harmful to the legitimate interests of their businesses users and, indirectly, also of consumers in the Union*"[38]. The superiority of service providers (online platforms) has the economic dependence as basis; „*they might unilaterally impose on business users practices which grossly deviate from good commercial conduct, or are contrary to good faith and fair dealing*"[39]. This way, the definition of the unfair contractual term between professionals/traders is taken from the proposal for a Regulation on a Common European Sales Law, which in article 86.1 (b) provides that: *"In a contract between traders, a contract term is unfair for the purposes of this Section only if: (b) it is of such a nature that its use grossly deviates from good commercial practice, contrary to good faith and fair dealing".*

It seems that the European legislator "saw" that not only do adherents, as consumers, need protection from unfair terms, but also professionals, as adherents, may need protection when contracting with other professionals in a position of power (economic, financial, informational, etc.). The P2B Regulation could be

[33] C. Rinaldo, *Beyond Consumer Law – Small Enterprises, Independent Contractors and other Professional Weak Parties,* in European Review of Contract Law, vol. 15, no. 2/2019, p. 236, https://doi.org/10.1515/ercl-2019-0012, accessed 20.10.2021.

[34] C.T. Ungureanu, *Drept internațional privat european în raporturi de comerț internațional*, Hamangiu Publishing House, Bucharest, 2021, pp. 33-37.

[35] I. Graef, *op. cit*, p. 451.

[36] Part of the analysis was taken from the author's article *Calificarea europeană a acțiunii în răspundere civilă intentată împotriva unui cocontractant și efectele acesteia. Cauza CJUE C-59/19*, in the Scientific Annals of "Alexandru Ioan Cuza" University, Juridical Sciences Series, Tome LXVI/II, 2020, pp. 112-115, [Online] at http://pub.law.uaic.ro/ro/volume-publicate/2020/anale-uaic-tomul-lxvi-tiine-juridice-nr.-2, accessed 19.11.2021.

[37] OJ, L 186/57, 11.7.2019.

[38] Recital 2 from the P2B Regulation.

[39] *Idem.*

considered as a first European instrument that raises the issue of protecting professionals who adhere to adhesion contracts concluded with online platforms.

The provisions of the Regulation are *overriding mandatory rules*[40], as they apply *irrespective of the law otherwise applicable.* [article 1(2)]. The sanction of non-compliance with the provisions of the P2B Regulation regarding the terms and conditions (contractual clauses) imposed on the users of the platform is their nullity [article 3(3)].

Another European instrument aimed at protecting agricultural and food professionals is Directive (EU) 2019/633 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain[41], which was to be transposed in the Member States by 1 May 2021[42] and which aims at *"combating practices that grossly deviate from good commercial conduct, that are contrary to good faith and fair dealing and that are unilaterally imposed by one trading partner on another"* [article 1(1)]. Thus, the Directive's goal is formulated almost identically to article 86 of the Regulation proposal on a Common European Sales Law.

The core motivation for the protection of professionals, parties to contracts in the agricultural and food supply chain, is the *imbalances in their bargaining power*[43], which can lead the more important and powerful trading partners to using unfair trade practices to their advantage; for example, they may "impose an unjustified and disproportionate transfer of economic risk from one trading partner to another" or "impose a significant imbalance of rights and obligations on one trading partner"[44].

In certain European national legislations, professionals also benefit from protection against unfair terms in B2B contracts.

Germany and France have in recent years drafted rules on unfair terms applicable to contracts between professionals with a view to making their

[40] For details on overriding mandatory rules, see C.T. Ungureanu, *Overriding Mandatory Rules in International Commercial Contracts Dispute Resolution. A Romanain perspective*, Cuadernos de Derecho Transnacional (Octubre 2020), Vol. 12, Nº 2, pp. 784-794, https://doi.org/10.20318/cdt.2020.5630, [Online] at https://e-revistas.uc3m.es/index.php/CDT/about/editorialPolicies#custom-0, accessed 19.11.2021.

[41] JO L111/59, 25.4.2019.

[42] At 18.11.2021, Romania has not yet transposed the directive. Nevertheless, a draft Law (PL-x no. 178/2021 on unfair commercial practices between enterprises in the agricultural and food supply chain, [Online] at http://www.cdep.ro/ pls/proiecte/upl_pck2015.proiect?cam=2&idp=19294, accessed, 18.11.2021) from June 3rd, 2021 is following the legislative procedure.

[43] H. Schebesta, K.P. Purnhagen, B. Keirsbilck, T. Verdonk, *Unfair Trading Practices in the Food Chain: Regulating Right?*, 2018, http://dx.doi.org/10.2139/ssrn.3267118, [Online] at https://ssrn.com/abstract=3267118, accessed 11.11.2021.

[44] Recital 1 from the Directive.

regulations attractive on the "market" of the law applicable to international contracts[45].

Germany has enacted rules since 1976[46] on judicial control over unfair terms in B2B contracts[47], integrated into the Civil Code in 2002. According to article 307 (1) of the German Civil Code, the clauses of standard B2B contracts *do not produce effects* if, contrary to good faith, they unreasonably benefit to the party who proposed them, including if they are unclear and difficult to understand[48]. These provisions have general applicability, regardless of the quality of the contracting parties, regardless of their bargaining power. The party that pre-drafted the contractual clauses must prove that the negotiation of the clauses has taken place (so the burden of proof is reversed), in order to avoid the application of the protective rules[49]. In legal practice, it is considered that the negotiation of a clause took place only when the adherent was available for negotiation and the stipulant gave him the opportunity to influence the content of the clause as to protect his economic interests; the bargaining power of the parties is not a criterion that the courts take into account[50].

The German approach to unfair terms in B2B contracts has been criticized in the legal literature, where it was considered that the protection of the adherent has gone too far, producing negative consequences. For instance, companies of German nationality, with great economic power, have chosen to change their headquarters, migrating to Switzerland, where the legislation does not contain such invasive provisions on the control of unfair terms[51].

In France, after the amendment of the Civil Code in 2018, the adhesion contract is defined in art. 1110, as the contract containing a set of non-negotiable clauses, predetermined by one of the parties[52] (the negotiable contract being the one in which its terms are negotiable).

---

[45] F.P. Patti, *Unfair Terms Control in Business-to-Business Contracts,* in The Italian Law Journal, vol. 5, no. 2/2019, pp. 584-585, https://doi.org/10.23815/2421-2156.ITALJ, [Online] at https://www.theitalianlawjournal.it/patti/, accessed 19.11.2021.

[46] *Act concerning the Regulation of Standard Contract Terms*, with comments by O. Sandrock, *The Standard Terms Act 1976 of West Germany*, in The American Journal of Comparative Law, vol. 26, no. 4/1978, p. 551, https://doi.org/10.2307/840058.

[47] F.P. Patti, *op. cit.*, p. 585.

[48] [Online] at https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p0915, accessed 08.11.2021. For comments see, H. Schulte-Nölke, *No Market for 'Lemons': On the Reasons for a Judicial Unfairness Test for B2B Contracts,* in European Review of Private Law, no. 2/2015, pp.195–216.

[49] C. Rinaldo, *op. cit.,* p. 230.

[50] *Ibidem.*

[51] *Idem*, p. 231.

[52] Article 1110 French Civil Code: *«Le contrat de gré à gré est celui dont les stipulations sont négociables entre les parties. Le contrat d'adhésion est celui qui comporte un ensemble de clauses non négociables, déterminées à l'avance par l'une des parties. »*, [Online] at https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070721/LEGISCTA000006090271/#LEGISCTA000006090271, accessed 08.11.2021.

In the legal literature it has been stated that it is not necessary for the qualification of a contract as negotiable that the clauses have been negotiated, but only to be susceptible to negotiation[53]. Determining the non-negotiable nature of a contractual clause could be very difficult in legal practice[54].

The ineffectiveness of unfair contractual terms has become a rule in French law, as art. 1171 of the French Civil Code[55] reads that, in an adhesion contract, *any non-negotiable clause,* predetermined by one of the parties, which creates a significant imbalance between the rights and obligations of the contracting parties, is *deemed unwritten.*

Also in France, following the amendment of the Commercial Code in 2019[56], article L 442-1, I.2° stipulates that any professional who carries out production, distribution or service activities and who imposes or tries to impose obligations on the other contracting party (also a professional), which creates a significant imbalance between the rights and obligations of the parties, is held liable and is obliged to repair the damage thus caused. According to art. L 442-4 I., the injured party (or anyone justifying an interest) may request the competent court *to cease the abusive practices* and *repair the damage.* The victim of abusive practices may request the *nullity of contractual clauses* or *illegal contracts* and the recovery of contributions[57]. These rules are not an absolute novelty for the French law. In 2008 an article was introduced in the Commercial Code, article 442-6, I, which stipulated the liability of the professional for subjecting or attempting to subject a trading partner to obligations creating a significant imbalance between the rights and obligations of the contractual parties[58].

In this context, the French legal literature[59] has raised the issue of the new amendments clarity, as the provisions of the Civil Code and of the Commercial

---

[53] A.W. Grumberg, F. Barrière, G. Roche, *Contrats d'adhésion et clauses abusives : un clair-obscur pour la pratique sociétaire*, in Fusions & Acquisitions Magazine, novembre-décembre 2018, p. 106.

[54] *Ibidem.*

[55] Article 1171 French Civil Code: *« Dans un contrat d'adhésion, toute clause non négociable, déterminée à l'avance par l'une des parties, qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite. L'appréciation du déséquilibre significatif ne porte ni sur l'objet principal du contrat ni sur l'adéquation du prix à la prestation. »*, [Online] at https://www.legifrance.gouv.fr/codes/ article_lc/ LEGIARTI000036829836/, accessed 06.11.2021.

[56] Modified by the *Ordonnance n°2019-359 du 24 avril 2019* - article 2, [Online] at https://www.legifrance.gouv.fr/codes/id/LEGIARTI000038414278/2020-11-28/?isSuggest=true, accessed 02.11.2021.

[57] [Online] at https://www.legifrance.gouv.fr/codes/id/LEGIARTI000038414278/2020-11-28/?isSuggest=true, accessed 02.11.2021.

[58] The original text: «[…]de soumettre ou de tenter de soumettre un partenaire commercial à des obligations créant un déséquilibre significatif dans les droits et obligations des parties» as referred to in X. Henry, *Clauses abusives dans les contrats commerciaux : état des lieux dix ans après*, in *AJ Contrats d'affaires : concurrence, distribution*, Dalloz, 2018, p. 370.

[59] X. Henry, *op. cit.*, pp. 372-373.

Code overlap, making it difficult to discern, all the more in legal practice, whether the general rule applies (from the Civil Code) or the special rule (from the Commercial Code).

In Belgium, after the amendment of the Economic Law Code in 2019, the unfair terms in B2B contracts[60] were prohibited, through the provisions of article VI.91/3, in force since December 1, 2020[61]. According to it, any contractual clause, concluded between undertakings (professionals), is abusive if, alone or in conjunction with one or more clauses, creates a *manifest imbalance* between the rights and obligations of the parties. The unfairness of the clause should be assessed on the basis of the nature of the products as object of the contract and on all circumstances existing at the time of the conclusion of the contract, on the general economics of the contract, the applicable commercial customs, and on all other contractual clauses or on another contract which the contract in question depends on and on the clarity and comprehensibility of the clause. The following two articles list the unfair terms and the presumed (irrefutably) unfair terms (article VI.91/4, article VI.91/5); art. VI.91/6 sets out the sanction for unfair terms in B2B contracts, namely the *(partial) nullity*[62].

Under Dutch law, the unfair standard terms are regulated in the Civil Code[63], in article 6:231-6:247, some of the provisions being of general applicability, and others being intended only for consumer contracts[64].

In Romanian law, so far, the only rule for unfair contractual terms between professionals is found in Law no. 72/2013 on measures to combat the delay in the performance of obligations to pay sums of money resulting from contracts concluded between professionals and between them and contracting authorities[65]. According to article 12, if the time limit for payment or the level of interest or additional damages are manifestly unfair for the debtor, then that certain clause is

[60] For an analysis see, D. Philippe, *Les clauses abusives dans les relations B2B*, 2019, [Online] at https://philippelaw.eu/wp-content/uploads/2019/08/Clauses-abusive4.pdf, accessed 06.11.2021.

[61] [Online] at http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?language=fr&la=F&cn=2013022819&table_name=loi&caller=list&F=&fromtab=loi&tri=dd%20AS%20RANK&rech=1&numero=1&sql=%28text%20contains%20%28%27%27%29%29#Art.VI.1, accessed 02.11.2021.

[62] Article VI.91/6 Economic Law Code: *«Toute clause abusive est interdite et nulle. Le contrat reste contraignant pour les parties s'il peut subsister sans les clauses abusives»*, [Online] at http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?language=fr&la=F&cn=2013022819&table_name=loi&caller=list&F=&fromtab=loi&tri=dd%20AS%20RANK&rech=1&numero=1&sql=%28text%20contains%20%28%27%27%29%29#Art.VI.1, accessed 02.11.2021.

[63] [Online] at http://www.dutchcivillaw.com/civilcodebook066.htm, accessed 10.11.2021.

[64] For an analysis see, A. Radonjić, *Unfair Contract Terms in SMEs in BW and draft CC of Serbia*, in Foreign Legal Life, 2017, p. 239 et seq.

[65] O.G. no. 182, 02.04.2013.

considered abusive and is struck by absolute nullity (article 15. 1), which may lead to compensation (article 15.2)[66].

Conclusions

"The massive emergence of technology in the realm of contracts and contract law has been interpreted mainly in terms of transaction costs reduction, since technology is instrumental to form agreements in a more expeditious way, regardless of the distance between contractors"[67].

The adhesion contract is an absolutely necessary tool in today's global trade. Beyond the benefits it offers, the contracting parties must also bear its inherent risks. However, a legislative intervention is necessary, with the main purpose of restoring the balance of power and thus the rights and obligations of the contracting parties and thereby ensuring a predictable market, characterized by fair trade and fair competition. The current rules show that the way forward has already been set at the European level. There is an expectation that the European instruments on unfair clauses in B2B contracts will give momentum at national level, in all member states, as well.

References

Bacon, J., Michels, J.D., Millard, C., Singh, J., *Blockchain Demystified*, Queen Mary School of Law Legal Studies Research Paper No. 268/2017

Baudouin, R., *Code civil du Québec annoté*, tome II, 14th Edition, Wilson & Lafleur Itée, 2011

Bercea, L., *Acțiunile colective în eliminarea clauzelor abuzive din contractele standard de consum. Cui prodest?*, in Revista Română de Drept Privat, no. 3/2013, pp. 24-36

Browne, N., Biksacky, L., *Unconscionability and the Contingent Assumptions of Contract Theory*, Michigan State Law Review, 2013, pp. 212- 255

D'Agostino, E., *Contracts of Adhesion Between Law and Economics. Rethinking the Unconscionability Doctrine*, Springer, 2015, ebook

Durovic, M., Lech, F., *The Enforceability of Smart Contracts*, The Italian Law Journal, vol. 5, no. 2/2019, pp. 493-511, https://doi.org/10.23815/2421-2156.ITALJ

Gaudemet, S., *La clause réputée non écrite*, Editions Economica, Paris, 2006

Goicovici, J., *Dreptul consumației*, Sfera Juridică, Cluj-Napoca, 2006

Gordley, J., *In defense of Roman contract law*, in Monateri, P. G. (ed.), *Comparative Contract Law*, Edward Elgar Publishing, 2017

Graef, I., *Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence*, in Yearbook of European Law, Vol. 38, no. 1/2019, pp. 448–499, https://doi.org/10.1093/yel/yez008

Granieri, M., *Technological contracts*, in Monateri, P.G., (ed.), *Comparative Contract Law*, Edward Elgar Publishing, 2017

[66] For details see, Ghe. Piperea, *Clauze și practici abuzive în relațiile dintre profesioniști*, 2013, [Online] at https://www.juridice.ro/256771/clauze-si-practici-abuzive-in-relatiile-dintre-profesionisti.html, accessed 02.11.2021.

[67] M. Granieri, *Technological contracts*, in P.G. Monateri (ed.), *Comparative Contract Law*, Edward Elgar Publishing, 2017, ebook, p. 408.

Grumberg, A.W., Barrière, F., Roche, G., *Contrats d'adhésion et clauses abusives : un clair-obscur pour la pratique sociétaire*, in Fusions & Acquisitions Magazine, novembre-décembre 2018

Guillemard, S., Onguene Onana, D.É., *Le contrat d'adhésion : actualités et droit international privé*, Les Cahiers de droit, Vol. 48, no. 4/2007, pp. 635–680. https://doi.org/10.7202/043948aradresse copiée

Henry, X., *Clauses abusives dans les contrats commerciaux : état des lieux dix ans après*, in *AJ Contrats d'affaires : concurrence, distribution*, Dalloz, 2018

Hesselink, M.W., *Unfair Terms in Contracts Between Businesses*, in Stuyck, J., Schulze, R. (eds.), *Towards a European Contract Law*, Sellier European Law Publishers, 2011, pp. 131-148

Király, M., *The Rise and Fall of Common European Sales Law,* in Elte Law Journal, no. 2/2015, pp. 31-42

Lefebvre, B., *Le contrat d'adhésion,* in „La Revue du Notariat", Montréal vol. 105, September 2003, pp. 439–490, https://doi.org/10.7202/1045922ar

Moise, A.-A., *Sources of Obligations*, in *The New Civil Code. Comments on articles*, C. H. Beck Publishing House, Bucharest, 2012

Norris, K., *Common European Sales Law: A Missed Opportunity or Better Things to Come,* in Business Law Review, vol. 37, no. 1/2016, pp. 29-32

Patti, F.P., *Unfair Terms Control in Business-to-Business Contracts,* in The Italian Law Journal, vol. 5, no. 2/2019, pp. 581-611, https://doi.org/10.23815/2421-2156.ITALJ

Philippe, D., *Les clauses abusives dans les relations B2B*, 2019

Piperea, Ghe., *Clauze şi practici abuzive în relaţiile dintre profesionişti*, 2013

Pop, L., *Tratat de drept civil. Obligaţiile. Vol. II. Contractul*, Universul Juridic Publishing House, Bucharest, 2009

Popa, I.-F., *„Tirania" clauzelor neuzuale*, Revista Română de Drept Privat, no. 1/2016

Radonjić, A., *Unfair Contract Terms in SMEs in BW and draft CC of Serbia*, in Foreign Legal Life, 2017, pp. 239-251

Rinaldo, C., *Beyond Consumer Law – Small Enterprises, Independent Contractors and other Professional Weak Parties,* in European Review of Contract Law, vol. 15, no. 2/2019, pp. 227-250, https://doi.org/10.1515/ercl-2019-0012,

Rodriguez-Yong, C.A., *The Doctrines Of Unconscionability And Abusive Clauses: a Common Point Between Civil And Common Law Legal Traditions,* Oxford University Comparative Law Forum, 2011

Rühl, G., *Smart (legal) contracts, or: Which (contract) law for smart contracts?,* March 10, 2020, in Cappiello, B., Carullo, G. (eds.), *Blockchain, Law and Governance*, Springer

Sandrock, O., *The Standard Terms Act 1976 of West Germany*, in The American Journal of Comparative Law, vol. 26, no. 4/1978, pp. 551-572, https://doi.org/10.2307/840058,

Schebesta, H., Purnhagen, K.P., Keirsbilck, B., Verdonk, T., *Unfair Trading Practices in the Food Chain: Regulating Right?,* 2018, pp. 690-700, http://dx.doi.org/10.2139/ssrn.3267118,

Schulte-Nölke, H., *No Market for 'Lemons': On the Reasons for a Judicial Unfairness Test for B2B Contracts,* in European Review of Private Law, no. 2/2015, pp.195–216

Scott, R.E., Choi, S.J., Gulati, M., *Revising Boilerplate: A Comparison of Private and Public Company Transactions*, Wisconsin Law Review, 2020, pp. 629-655

Tutt, A., *On the Invalidation of Terms in Contracts of Adhesion*, Yale Journal on Regulation, vol. 30, no. 2/2013, pp. 439-474

Ungureanu, C.T., *The Romanian Adherent, Party to the Transnational Adhesion Contract,* in *Studies of Business Law - Recent Developments and Perspectives*, Peter Lang, Berlin, 2013, pp. 261-285

Ungureanu, C.T., *Drept international privat european în raporturi de comerţ international*, Hamangiu Publishing House, Bucharest, 2021

Ungureanu, C.T., *Overriding Mandatory Rules in International Commercial Contracts Dispute Resolution. A Romanain perspective*, Cuadernos de Derecho Transnacional (Octubre 2020), Vol. 12, Nº 2, pp. 784-794, DOI: https://doi.org/10.20318/cdt.2020.5630

Virassamy, G., *Les contrats de dépendance, essai sur les activités professionnelles exercées dans une dépendance économique*, Librairie Générale de Droit et de Jurisprudence, Paris, 1986

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-2

Munca şi noile ei contururi

Labour and Its New Contours

Raluca Dimitriu[1]

Rezumat: Doctrina caută de decenii separarea raporturilor de muncă de muncă de alte tipuri de raporturi juridice, cu scopul identificării obiectului dreptului muncii. Prezentul studiu merge un pas mai departe, încercând să identifice o definiţie a muncii însăşi. Asemeni universului în care trăim, şi universul digital este în expansiune, iar munca tinde să se disipeze în sutele de activităţi pe care le desfăşurăm zilnic, fără a mai exista o barieră fermă între ce anume este şi ce anume nu este propriu-zis muncă. Iar uneori considerarea unei activităţi ca nefiind muncă poate constitui o formă subtilă de exploatare. Nu mai este necesar ca beneficiarul muncii să îl plătească prost sau să nu îl plătească deloc pe cel care munceşte, nu mai este necesar să deghizeze contractul de muncă într-un alt contract; este suficient să îl convingă pe lucrător că, de fapt, ceea ce face el nu e muncă deloc.Voi încerca să explic această mutaţie şi să definesc câteva criterii de identificare a muncii.

Cuvinte-cheie: lucrător; dreptul muncii; digitalizare; istoria muncii

Abstract: The doctrine has been trying for decades to separate labour relations from other types of legal relations, with the purpose of identifying the object of Labour Law. Through the present study, we take a step forward, trying to identify a definition of labour itself. Similar to the universe we live in, the digital environment is also expanding, and „labour” tends to dissipate in the hundreds of activities we carry out every day, without any firm barrier between what is and what is not labour in itself. Moreover, sometimes, considering an activity as „not labour” can be a subtle form of exploitation. It is no longer necessary for the beneficiary of work to underpay or not to pay at all the person who is working; it is not necessary for the beneficiary of work to disguise the employment contract in another legal figure; it is sufficient to persuade the worker that, in fact, what she does in not work at all. I will attempt to explain this alteration, contouring at the same time several criteria for the identification of work.

Keywords: worker; labour law; digitization; the history of work

1. Introducere. Munca – un construct cultural

La prima vedere, munca pare un concept peren. Schimbătoare sunt raporturile juridice în baza cărora se prestează aceasta, dar actul în sine de a munci pare clar delimitat de orice altă activitate. De aceea, majoritatea cercetătorilor s-au

[1] Profesor univ. dr., Academia de Studii Economice, Bucureşti, e-mail: raluca.dimitriu@drept.ase.ro

concentrat mai ales asupra diferenţierii muncii prestate într-un raport de subordonare de cea prestată în temeiul unui contract civil, în încercarea de identificare a graniţelor dreptului muncii. Aceste graniţe sunt în mişcare, dreptul muncii pierzând adesea teren prin falsa etichetare a unora dintre lucrători ca fiind „independenţi", ceea ce a generat o extinsă literatură de drept al muncii menită tocmai să identifice criteriile muncii dependente şi să recupereze raporturile contractuale pierdute prin astfel de contracte deghizate. Tehnologia informaţiilor şi a comunicaţiilor este doar o unealtă, aşa cum multe unelte s-au succedat în timp. Indiferent de uneltele folosite, s-a spus, munca rămâne muncă, astfel încât interesul cercetătorului ar trebui să fie concentrat asupra raportului contractual în baza căruia este aceasta prestată.

Dar dacă nu numai munca dependentă, ci munca însăşi ar fi în schimbare? Dacă tehnologia nu ar fi doar un adjuvant, o modalitate în care munca se prestează, diferit doar formal de instrumentele folosite până acum, ci ar constitui sursa unei mutaţii esenţiale în însăşi definiţia muncii? Mai corespund definiţiile tradiţionale ale muncii contextului tehnologic şi social actual? Pentru a răspunde – fie şi parţial – la astfel de întrebări, vom trece în revistă diferitele etape istorice în definirea muncii şi raportarea socială la aceasta. Nu o vom face sistematic şi aplicat, ci pasager, doar cu scopul de a dovedi faptul că munca este un construct cultural, şi că nici definiţia acesteia, nici percepţia socială asupra muncii nu sunt constante în timp. Deşi în toate vremurile, în mentalul colectiv hărnicia a fost valorizată pozitiv, prin opoziţie cu trândăvia, ce anume, în mod concret, constituie muncă – a suferit schimbări continue. Vom vedea astfel că religia, revoluţia industrială şi, acum, cea digitală – au avut un anume impact asupra acestui construct. Vom căuta tot astfel unele criterii în funcţie de care să deosebim munca, în contextul actual, de alte activităţi. Şi vom semnala unele dintre efectele juridice ale acestor evoluţii.

2. Iniţial...

În societăţile timpurii, munca nu era foarte clar separată de celelalte sfere ale vieţii private. Nu se produsese încă divorţul dintre muncă şi viaţa de familie sau viaţa religioasă[2] iar activităţile necesare obţinerii de resurse nu erau privite ca fiind diferite de celelalte interacţiuni sociale[3]. Munca se desfăşura în comun, iar refuzul de a munci era sancţionat cu ostracizarea. Oamenii nu erau plătiţi pentru a munci; munca era o activitate naturală şi inevitabilă.

Odată cu apariţia societăţilor organizate mai complex, munca a început să se separe de celelalte activităţi, şi chiar tipurile de muncă au început să fie prestate de oameni diferiţi. A apărut specializarea muncii.

[2] H. Applebaum, *The Concept of Work. Ancient, Medieval, and Modern*, State University of New York Press, 1992, pp. 9-10.

[3] S. Zuboff, *The Work Ethic and Organization*, în J. Barbash, R.J. Lampman, S.A. Levitan, G. Tyler (coordonator), "The Work Ethic: A Critical Analysis", Industrial Relations Research Association, Madison, WI, 1983, p. 153.

Cu timpul însă, munca a început să fie disociată de activităţile superioare, cele dedicate gândirii şi folosofiei. Aristotel, la fel ca mulţi dintre gânditorii greci, considera că munca interferează cu îndatoririle cetăţenilor şi îi distrage de la activităţi mai virtuoase precum politica, arta şi filozofia[4]. Acestea nu puteau fi stăpânite decât printr-o educaţie îndelungată care necesită timp şi – fireşte - timp liber.

O lungă perioadă de timp, munca plătită a avut caracter ocazional şi marginal, societăţile întemeindu-şi necesarul de producţie pe munca sclavilor, devenită o parte importantă a economiei (mai ales în sec. V – III î.Hr. pentru Grecia şi sec. I î. Hr – sec. II d. Hr. pentru Roma), şi merită subliniat că munca lor nu era numai necalificată sau grea: sclavii desfăşurau şi activităţi intelectuale sau administrative. Astfel încât percepţia asupra muncii (de toate felurile) a devenit – prin contaminare - negativă; munca a început să fie privită cu un anume dezgust. Războiul şi politica erau îndeletniciri legitime ale cetăţenilor, dar asta deoarece ele nu erau percepute ca muncă; munca în sine era însă rezervată sclavilor şi necetăţenilor[5]. Munca îl coboară sau chiar îl înjoseşte pe om, credeau romanii în perioada imperiului, şi cred că aceştia ar fi fost foarte miraţi de valoarea pozitivă care avea ulterior să îi fie asociată muncii. În mod deosebit, a munci pentru altul era degradant şi umilitor. Pentru Cicero, munca plătită are vulgară şi nepotrivită pentru un cetăţean; plata muncii nu este altceva decât o formă de sclavaj. Iar Seneca spunea că, dacă printr-o neferită împrejurare a sorţii, ar ajunge să muncească, n-ar face o dramă din asta. Doar s-ar sinucide...[6]

3. Impactul religiei asupra muncii

Percepţia socială asupra muncii avea să fie ulterior puternic influenţată de religie. În creştinism, munca este blestem originar ("În sudoarea frunţii tale îţi vei mânca pâinea ta, până te vei întoarce în pământul din care eşti luat; căci pământ eşti şi în pământ te vei întoarce" - Facerea 3:19), dar şi datorie creştină; Sfântul Apostol Pavel spune de exemplu că „dacă cineva nu vrea să lucreze, acela nici să nu mănânce" (II Tes. 3, 10). În Evanghelia după Matei, Isus li se adresează în mod direct direct celor ce muncesc: „Veniţi la Mine, toţi cei trudiţi şi împovăraţi, şi Eu vă voi da odihnă" (Matei, 11:28).

Aceasta este o schimbare notabilă, care a dus la reconsiderarea muncii şi a celor ce o prestează. Deşi există un imens univers de nuanţe. În Calvinism, munca este o formă de glorificare a lui Dumnezeu, în timp ce Ortodoxia menţine o anume

[4] P.D. Anthony (coordonator), *The Ideology of Work*, Tavistock Publications, 1977, p. 17.

[5] Și aici nu intră doar munca manuală, ci chiar și activitățile intelectuale. Pentru Cicero, chiar și ocupații ca cea de doctor, arhitect sau profesor erau considerate nepotrivite pentru un cetățean. Singura excepție o formau juriștii, datorită legăturii cu activitatea politică, socotită onorabilă. H. Applebaum, *op. cit*, p. 96.

[6] După cum arată cu umor E. Carrère, în *Împărăția cerurilor*, Editura Trei, Bucureşti, p. 205.

distanţare faţă de aceasta[7], esenţa umană fiind socotită a fi mai curând contemplativă, „duminicală” [8].

În Islam, devotamentul religios nu scuteşte credinciosul de muncă. Munca este considerată în centrul vieţii religioase[9], fiind considerată concordantă cu comportamentul spiritual prescris şi privită uneori chiar ca formă de rugăciune (*ibadah*)[10], atâta timp cât nu este prestată pentru faimă sau autoafirmare.

Raportarea la muncă se face în mod diferenţiat, în funcţie de ocupaţie.

Astfel, religia dictează tipul de muncă pe care fiecare individ are posibilitatea de a o presta, iar sistemele religioase au introdus obstacole diverse în practicarea anumitor meserii. În hinduism, de exemplu, castele sunt grupări ierarhice rigide, fiecăreia fiindu-i destinată o ocupaţie specifică: Brahmanii sunt preoţi şi învăţaţi, Kshatriyas sunt militari şi administratori, Vaishyas sunt comercianţi şi artizani, iar Shudras sunt muncitori manuali. Ca urmare, multe dintre profesii sunt inaccesibile castelor inferioare. Fiecăreia dintre caste – cărora li se adaugă „cei de neatins”, în afara sistemului – îi corespunde aşadar un anumit tip de muncă, iar alegerea liberă a profesiei este chiar şi astăzi, în unele regiuni, deşi posibilă juridic, imposibilă din cauza restricţiilor culturale.

În religia creştină, cele mai multe meserii şi ocupaţii sunt ocrotite de câte un sfânt (spre exemplu, arhitecţii şi constructorii sunt protejaţi de către Sfântul

[7] Părintele Serghie Sevici (1903-1987) afirma: „Nu-i rău că truda nu-ți aduce nicio bucurie. Că n-am venit pe lume ca sa ne desfătăm. Ci suferința-i zestrea noastră pământească. Ba, rău este sa-ți placă munca ta, să-ți faci din ea un idol, să-i dai tot sufletul tău, lăsând de o parte ce e cu adevărat de preț. Veselie să-ți aducă lucrarea celor duhovnicești. Iar munca să-ți fie nevoință, spre încercare, cum este pentru călugăr ascultarea care-l rupe de la rugăciune și slujbe. Socotește-o uneltitoarea răbdării, că multă răbdare cere munca.”, [Online] la https://www.crestinortodox.ro/editoriale/munca-este-nefireasca-140821.html, accesat 1.10.2021.

Munca poate fi un mijloc, dar niciodată un scop în sine: „Apoi, când m-am uitat cu băgare de seamă la toate lucrările pe care le făcusem cu mâinile mele şi la truda cu care le făcusem, am văzut că în toate este numai deşertăciune şi goană după vânt şi că nu este nimic trainic sub soare.” (Eclesiastul, 2:11).

[8] V. Mureşan, *Muncă şi libertate*, în România culturală, anul 4, numărul 73, 16-30 noiembrie 2009, [Online] la http://www.romaniaculturala.ro/images/articole/muresan73verso09.pdf, accesat 1.10.2021: „Noi suntem oferiţi unei «Duminici» a libertăţii contemplative”, arată autorul. Munca „ne decade din vocaţia noastră supremă: contemplaţia”.

Această reticență față de valoarea spirituală a muncii poate fi întâlnită și la autori aparținând altor spații și epoci, cum ar fi Henry David Thoreau, care spunea în 1837, în *Commencement Essay* că „ar trebui ca ordinea lucrurilor să fie răsturnată; o zi pe săptămână să fie cea de trudă, prin care omul să-și câștige traiul cu sudoarea frunții, iar celelalte șase să fie Sabat, în care omul să se bucure de revelațiile Naturii” (Bloom’s Literary Criticism, 2008, p. 75).

[9] A.J. Ali, A. Al-Owaihan, *Islamic work ethic: a critical review*, Cross Cultural Management: An International Journal, Vol. 15 No. 1, 2008, pp. 5-19, https://doi.org/10.1108/13527600810848791, p. 7, accesat 1.10.2021.

[10] I. Ahmad, *Islamic Labour Code*, [Online] la https://islamiclabourcode.org/work-ethic-and-islam/, accesat 1.10.2021.

Apostol Toma, minerii – de către Sfânta muceniţă Varvara, lucrătorii în piatră de către Sfântul Clement, doctorii de către Sfinţii Cosma şi Damian, pictorii de către Sfântul evanghelist Luca, meşteşugarii de către Sfântul Iosif etc.)

Cât priveşte însă obligaţia de plată a muncii, aici întâlnim abordări similare în marile religii. Profetul Mohamed afirma că va pleda personal împotriva celui care a beneficiat de munca unui lucrător, fără a-l plăti, recomandând, într-un *hadis* foarte expresiv, „Plăteşte-i lucrătorului salariul înainte ca transpiraţia să i se usuce". În creştinismul ortodox, „oprirea plăţii lucrătorilor" este un păcat „strigător la cer".

În întreaga perioadă pre-industrială, munca este prestată în familia lărgită, în comunitate; este prin ea însăşi un mod de comunicare şi socializare.

4. După revoluţia industrială

O mutaţie esenţială în ceea ce priveşte munca este adusă cu sine de revoluţia industrială, cu care conceptul de „etică a muncii" şi modul ulterior de raportare la muncă este cel mai adesea asociat. Etica muncii are înţelesul de „atitudine pozitivă faţă de muncă"[11] şi a fost deplin potenţată de etica protestantă. Munca a fost întotdeauna un mijloc pentru obţinerea celor necesare traiului, dar nu a avut până acum o valoare intrinsec morală.

A existat însă de la început o anumită ipocrizie în spatele de noţiunii de etică a muncii, mai ales în ceea ce priveşte marea masă a lucrătorilor săraci, pentru care munca era singurul mijloc de subzistenţă, astfel încât a apărut ca fiind necesară, cum s-a arătat[12], construcţia unui sistem de valorizare a muncii, cu tonuri teologice, pentru „justificarea" muncii.

În societatea occidentală, probabil cel mai important moment din perspectiva modului social de raportare la muncă l-a constituit Reforma. Ea adus cu sine conceptul de „etică a muncii", pe care îl întâlnim şi astăzi, deşi secularizat.

Dreptul tradiţional al muncii s-a construit pe fundamentul *fordist* al raportului de muncă. Este vorba despre construcţia juridică în temeiul căreia lucrătorul investeşte cea mai mare parte a vieţii sale adulte în întreprindere, care devine un element al identităţii sale. El lucrează pe parcursul unui program determinat, la sediul unităţii angajatoare, alături de colegii săi, cu care constituie sindicate şi alte modalităţi de organizare, participând astfel la negocierea colectivă, la greve şi acţiuni sociale. Acesta este contextul în care s-a creat dreptul muncii, alcătuit din dispoziţiile contractelor colective de muncă astfel încheiate şi din legislaţia standardelor minime, de protecţie a lucrătorului dezavantajat de subordonarea în care se găseşte în raport cu angajatorul său. În acest context, lucrătorul ajunge să se identifice în societate prin profesia sa, prin locul său de muncă – pe

[11] D.J. Cherrington, *The Work Ethic: Working Values and Values That Work*, New York: Amacom (1980), p. 19.

[12] G. Tyler, *The Work Ethic: a union view*, în J. Barbash, R.J. Lampman, S.A. Levitan, G. Tyler (coord.), *The Work Ethic: A Critical Analysis*, Industrial Relations Research Association, Madison, WI, (1983), p. 198.

care le percepe ca atribute generatoare de mândrie sau, dimpotrivă, de resentimente ori frustrare[13].

Observăm aşadar că societatea s-a raportat în timp în moduri diferite la muncă; sclavii nu aveau nevoie de motivaţii ideologice pentru a munci, fiind supuşi constrângerii fizice pentru a o face. În timp, constrângerea fizică a fost înlocuită cu cea religioasă şi, mai apoi, cu cea moral-seculară.

5. Astăzi...

Astăzi, societatea poziţionează munca drept determinantă pentru împlinirea personală. Întrebarea „ce vrei să te faci când vei fi mare?" pe care o aude astăzi aproape fiecare copil, ar fi surprins un observator provenit din secolele trecute, când ideile de „carieră" şi „succes profesional" nu-şi făcuseră încă loc în sfera preocupărilor cotidiene. Capacitatea de muncă şi angajabilitatea sunt scopurile principale ale sistemului de educaţie, ale oricărui tip de tratament medical, ale politicilor sociale, ale sistemelor de reintegrare socială din penitenciare sau ale programelor de compensare a şomajului[14]. Ceea ce urmăreşte societatea de la individ este ca acesta să fie apt de muncă.

Bineînţeles, activităţile necesare pentru susţinerea vieţii sunt fundamentale (omul întotdeauna a trebuit să mănânce). Dar munca, aşa cum o înţelegem astăzi, abstractizată, independentă de formele ei particulare (arat, construit, vânat, gătit) are origini moderne. Până acum câteva secole, aspiraţiile, succesul, scopul în viaţă sau sentimentul de identitate erau regăsite în tradiţii şi credinţă, nu în muncă[15].

Schimbarea accentului de pe muncă – în sensul de mijloc de asigurare a resurselor necesare traiului, pe muncă – în sensul de izvor de dezvoltare personală a modificat semnificativ percepţia socială generală asupra muncii. Protestantismul şi, cu deosebire Calvinismul, a sanctificat munca, socotind-o un ideal spiritual prin ea însăşi. Iar societatea de astăzi, centrată cumva în jurul muncii, nu face decât să urmeze acest model. El a pătruns din spaţiul occidental influenţând etica muncii şi în ţările care, pe fondul tradiţional ortodox, nu valorizau munca în context spiritual.

Tradiţional, dreptul muncii se ocupă de reglementarea muncii – a activităţii prestate în raport de subordonare. Scapă normelor de drept al muncii activitatea prestată în raporturi de egalitate juridică, care formează obiect al dreptului civil. Dar ne găsim astăzi pe teritoriul unui conflict negativ de competenţă: munca prestată de ne-salariaţi, care nu se găsesc însă în relaţii juridice de egalitate cu beneficiarul muncii nu este guvernată de dreptul muncii, nefiind prestată de salariaţi, dar nici propriu-zis dreptului civil, nefiind o muncă real independentă. Singura formulă juridică prin care aceste activităţi ar fi re-apropriate de dreptul

[13] R. Dimitriu, *Dreptul muncii. Anxietăți ale prezentului*, Editura Rentrop şi Straton, București, 2016, p. 18.

[14] N. Glazer, *Women's Paid and Unpaid Labor: The Work Transfer in Health Care and Retailing* (Women in the Political Economy), Philadelphia: Temple University Press, 1993, p. 33.

[15] B. Hunnicutt, *Work Is Our Religion And It's Failing Us*, Huffpost, 18 mai 2018, [Online] la https://www.huffpost.com, accesat 1.10.2021.

muncii ar fi cea a simulaţiei, atunci când se poate proba că în realitate contractul de muncă a fost deghizat într-un contract civil.

Problema este că există o serie de activităţi care nu sunt supuse niciunei reglementări. Ele nici nu sunt percepute ca fiind muncă, deşi produc profit unei anumite entităţi, iar la baza prestării lor se găseşte – uneori bine ascuns - un contract. Unele astfel de activităţi sunt sporadice, incidentale, astfel încât lipsindule elementul de repetabilitate care caracterizează îndeobşte munca, trec „pe sub radarul" analizei juridice. Altele sunt mai importante cantitativ, dar sunt de asemenea nereglementate mai curând din cauza dificultăţii de identificare a părţilor contractului pe baza căruia sunt prestate. În sfârşit, altele sunt nereglementate din cauza noutăţii lor, constituind expresia unor evoluţii tehnologice la care dreptul nu a reuşit încă să se adapteze.

6. Cum a schimbat digitalizarea conceptul de muncă

Cum arătam, conceptul modern de muncă a apărut odată cu revoluţia industrială, ca activitate plătită ce se desfăşoară într-un spaţiu diferit de propria gospodărie şi care este ferm separată de viaţa privată. Lucrătorul pleacă de acasă ca să muncească; în spaţiul destinat muncii dezvoltă relaţii sociale care sunt diferite de cele de familie, iar apoi se întoarce acasă pentru a-şi petrece timpul de repaus – un mod de organizare a vieţii ce nu exista înainte de revoluţia industrială.

Digitalizarea a adus însă cu sine o nouă mutaţie asupra modului de raportare la muncă. Aceasta nu mai este neapărat o experienţă colectivă, ci solitară. Graniţele dintre viaţa privată şi cea profesională sunt blurate, deja lucrătorul digital a încarnat activitatea productivă în programul petrecut cu familia şi puţini sunt cei care mai reuşesc să traseze limite ferme între aceste două universuri.

Asemeni lui Benjamin Button, cu trecerea timpului, munca pare a se întoarce spre propria sa copilărie.

Într-adevăr, iată că astăzi munca prestată în cadrul familiei, în propria gospodărie, a început să aibă o relevanţă pe care nimeni nu bănuia că o va recăpăta în contextul societăţii moderne. Depărtarea fizică de colegii săi, fenomen preexistent, dar fără îndoială accentuat de criza Covid 19, metodele manageriale contemporane, orientate spre autonomie, ca şi relaţia tot mai directă cu clientul, au transformat lucrătorul într-un lup singuratic, ce îşi obţine resursele într-un context universal concurenţial şi căruia i se pretinde o atitudine mai curând antreprenorială. Aproape nimic din ceea ce era definitoriu pentru munca prestată în cuprinsul marilor companii industriale, care a prilejuit geneza dreptului muncii pe fundamentul solidarităţii dintre lucrătorii ce lucrau umăr lângă umăr, nu mai este indispensabil astăzi. Dacă privim de exemplu R*ecomandarea* (nr. 198) din 2006 a *OIM* privind *relaţiile de muncă*, ca şi indicatorii socotiţi a fi determinanţi pentru identificarea unei relaţii de muncă, putem observa cât de mult s-a schimbat munca dependentă în ultimii 15 de ani.

Digitalizarea a schimbat nu numai modul în care munca este efectiv prestată, dar şi modul în care o percepem. Desprinderea de un spaţiu fizic de prestare a muncii poate conduce spre repoziţionarea muncii în întreaga noastră viaţă. Deja

generaţiile cele mai recent intrate pe piaţa muncii nu mai valorizează munca aşa cum o făceau părinţii lor, ci tind să aşeze în centrul existenţei lor timpul liber şi experienţele de viaţă (nu neapărat profesională).

7. Criterii de distingere a muncii de alte activităţi

Literatura abundă de definiţii date muncii[16]. În psihologia muncii, munca reprezintă totalitatea manifestărilor umane conştiente, mentale şi/sau operaţionale, prin care omul acţionează asupra mediului, asupra lui însuşi şi a celorlalţi oameni în vederea satisfacerii trebuinţelor, intereselor, aspiraţiilor, realizării unor scopuri. Caracteristicile muncii sunt: „(a) munca este o activitate învăţată: munca nu este un simplu răspuns al organismului la stimuli de moment sau la solicitări ale instinctului, ci o activitate de îndeplinire a unor sarcini; (b) prin muncă omul îşi produce bunurile materiale necesare subzistenţei şi pe cale spirituale, deci în consecinţă ea este un factor esenţial în procesul de umanizare, socializare şi culturalizare a fiinţei umane; (c) este o activitate deliberată întrucât atât produsul, rezultatul muncii cât şi scopul sarcinii de muncă au fost construite mai întâi în plan mental, cu participarea întregului sistemul psihic uman. Scopul este elementul esenţial care declanşează, susţine şi determină felul activităţii de muncă".[17]

Dar care sunt elementele unei definiţii a muncii, în contextul de astăzi, marcat de evoluţiile tehnologice pe care le aminteam?

Voi începe prin a preciza care sunt elementele pe care nu cred că ar trebui să le cuprindă o astfel de definiţie.

Tradiţional, când ne gândim la muncă, avem în vedere o activitate mai curând grea, care durează o perioadă îndelungată, care are caracter repetitiv, pe care o prestăm cel mai adesea nu din plăcere, ci din necesitatea de a obţine resursele necesare existenţei. Tindem să asociem aşadar munca efortului şi neplăcerii, excluzând activităţile pe care le desfăşurăm din pasiune. Cu toate acestea, munca creativă nu este cu nimic mai puţin muncă. Faptul că resortul principal al desfăşurării unei munci îl constituie pasiunea permite uneori beneficiarilor muncii creative să profite de efortul lucrătorilor (care nici nu percep activitatea depusă de ei ca pe un efort, ci ca pe o necesară formă de expresie). Excluderea acestor activităţi din sfera muncii constituie în fond o formă de exploatare. De aceea, în definiţia muncii, aş elimina aspectele ce ţin de modul de raportare psihologică la aceasta şi aş spune că e nerelevant dacă e grea sau uşoară, plăcută sau neplăcută, sau dacă se confundă sau nu cu pasiunea celui care o prestează. Cu atât mai mult cu cât tehnologia eli-

[16] Potrivit dicționarului explicativ al limbii române, munca este „desfășurare a unei activități fizice sau intelectuale îndreptată spre un anumit scop; activitate prin care omul modifică și adaptează lucrurile din natură pentru satisfacerea trebuințelor sale". Tot astfel, munca este definită ca fiind „activitatea specifică, manuală și/sau intelectuală, prin care oamenii își utilizează aptitudinile fizice și spiritual în scopul producerii bunurilor, prestării serviciilor și executării lucrărilor cerute de trebuințele lor". A se vedea, I.T. Ștefănescu, „Munca", în *Dicționar de dreptul muncii*, Editura Universul Juridic, Bucureşti, 2014, pp. 250-251.

[17] A se vedea A. Tabachiu, *Psihologia muncii* (curs), Editura Universităţii Politehnice, Bucureşti, 1997.

mină cele mai multe din atributele negative care au caracterizat în mod tradiţional munca.

În al doilea rând, munca trebuie diferenţiată de ocupaţie. Ea are o sferă mult mai largă, şi nu încorporează doar activităţile destinate obţinerii de venituri necesare traiului. O activitate nu încetează a fi muncă doar pentru că nu este prestată cu regularitate.

Nerelevantă este şi măsura în care munca este sau nu plătită. Munca prestată în baza unui contract de muncă voluntară este numaidecât muncă, iar caracterul gratuit al contractului nu îi poate schimba această calitate.

Apoi, munca nu ar trebui opusă odihnei. Multe activităţi, deşi obositoare, intră totuşi în sfera recreativă sau de divertisment. Aşa a apărut noţiunea de „odihnă activă", care presupune „desfăşurarea unor activităţi cu valenţe revitalizante sau alternarea unui fel de activitate cu altul"[18].

În sfârşit, nu cred că referire la „mijloace de producţie" mai este obligatorie în definirea muncii astăzi, când digitalizarea a permis detaşarea acesteia de cele mai multe elemente materiale şi deplasarea ei în sfera exclusiv virtuală.

Dimpotrivă, în definirea muncii cred că ar trebui cuprinse ca elemente definitorii:

a) Munca este o activitate învăţată. Ea nu este prestată pe baze instinctive. Cu toate acestea, procesul de învăţare nu intră în conceptul de muncă, constituind o etapă preliminară muncii propriu-zise. În mod ideal, munca fructifică învăţarea. Cu toate acestea, în cazuri speciale, cum ar fi cel al artiştilor învăţarea (studiul la instrument, de exemplu) poate fi cu greu separată de procesul de fructificare a acestui efort, astfel încât aici graniţele pot deveni invizibile.

b) Munca presupune o alocare deliberată a energiei[19]…

c) orientată către un scop. Scopul ar trebui să fie diferit de prestarea propriu-zisă a activităţii respective.

d) Munca se prestează în baza unui act juridic (adesea, un contract)...

e) şi este solicitată de o altă persoană sau folositoare unei alte persoane (nu numai lucrătorului). Cu privire la acest element putem însă întâlni excepţii, deoarece uneori munca nu este nici solicitată, nici folositoare la momentul la care este prestată, dar poate deveni astfel în timp. De exemplu, munca creativă este uneori prestată ca activitate voluptorie, din simpla dorinţă a artistului, fără să aibă la bază o ofertă contractuală. Ea va fi însă reconsiderată retroactiv, odată ce produsul muncii va forma obiect al unei astfel de oferte.

Aceste elemente vor putea sta la baza unei definiţii – fie şi provizorii – a muncii. Dar pornind de aici ne putem întreba: de ce ar fi necesar, din punct de vedere juridic, să definim munca? Să fie acesta un exerciţiu steril şi abstract?

Dimpotrivă. Definirea muncii şi determinarea graniţelor dintre aceasta şi alte tipuri de activităţi constituie o întreprindere fundamentală, mai ales în contextul

[18] G.M. Hosu, *Odihna activă*, [Online] la http://www.psihologsportiv.ro/recuperarea/odihna-activa/ accesat 1.10.2021

[19] J. Suzman, *Munca. O istorie a modului în care ne petrecem timpul* (trad. de Iulia Bertea-Nani), Editura Publica, Bucureşti, 2021, p. 18.

celor mai recente evoluţii tehnologice. Pentru că în realitate definiţiile tradiţionale ţin foarte puţin cont de aceste evoluţii.

Nu e vorba numai despre faptul că au apărut noi profesii, ci despre modul însuşi în care aceasta se prestează în prezent: crearea de conţinut online, activitatea desfăşurată de influenceri, recenziile la produsele cumpărate, activităţile desfăşurate în industria de jocuri – pot să constituie activităţi lucrative, care pot fi monetizate, chiar dacă cel mai adesea nu sunt monetizate chiar de lucrătorul însuşi. De altfel, uneori considerarea unei activităţi ca nefiind muncă poate constitui o formă subtilă de exploatare. Nu mai este necesar ca beneficiarul muncii să îl plătească prost sau să nu îl plătească deloc pe cel care munceşte, nu mai este necesar să deghizeze contractul de muncă într-un alt contract; este suficient să îl convingă pe lucrător că, de fapt, ceea ce face el nu e muncă deloc.

Să luăm de exemplu munca consumatorului. Ideea de „a-l pune pe consumator la muncă" nu este nouă: restaurantele McDonald's au transferat de mult clienţilor o parte din sarcinile de chelner[20], iar la Ikea încă de decenii obiectele de mobilier sunt asamblate de către cumpărători. Dar tehnologizarea a permis o amplificare a acestui mod al companiilor de a extrage muncă gratuită din partea clienţilor, prin cele mai diverse modalităţi: citirea codului de bare de pe produse şi plata fără ajutorul casierilor, achiziţionarea online de bilete de transport, de spectacol, de spaţii de cazare, self check in–ul în aeroport şi multe altele. Acest proces a permis producătorilor să reducă cheltuielile cu personalul şi a atras disponibilizări masive. Munca prestată de consumator conduce la crearea unei anume relaţii personale cu producătorul, mai ales atunci când consumatorul este implicat nu numai în prestaţii necalificate, ci chiar în elaborarea de strategii, în furnizarea de idei pentru viitoare produse ale firmei sau pentru căi de îmbunătăţire a celor existente. Consumatorul este implicat şi în politicile de personal ale producătorului, solicitându-i-se feedback după aproape fiecare interacţiune cu personalul acestuia.

Nu ne preocupă la acest punct dacă efectul s-a resimţit şi în scăderea preţului produselor şi serviciilor, altfel spus, dacă clienţii au şi fost recompensaţi în vreun fel pentru munca depusă: uneori da, alteori nu. Chiar dacă aportul clienţilor nu duce la scăderea preţului, acest fapt nu e neapărat relevant în sine: nu ar fi primul caz de muncă neplătită. Dar chestiunea esenţială, din perspectiva pe care o avem aici în vedere este că adesea clienţii nici nu percep aceste operaţii ca fiind muncă. Şi aici e problema: avem de a face cu un tip de prestaţie ce nu numai că nu face obiectul unei înţelegeri contractuale distincte de achiziţionarea efectivă a produsului sau a serviciilor, dar – poate şi pentru că vorbim despre activităţi uşoare, de scurtă durată, chiar agreabile – nici nu poate fi pusă în discuţie ca „muncă". Totuşi, dacă luăm în considerare criteriile pe care le-am propus la început – vom afirma fără tăgadă că activităţile consumatorului trebuie să intre în sfera

[20] D. Zwick, S.K. Bonsu, A. Darmody, *Putting Consumers to Work: 'Co-creation' and new marketing govern-mentality*, Journal of Consumer Culture, 2008; 8(2), pp. 163-196, https://doi.org/10.1177/1469540508090089, p. 166, accesat 1.10.2021.

conceptului de muncă. După cum s-a arătat, „the 'free labor' of consumers is simultaneously voluntarily given and unwaged, enjoyed and exploited"[21].

Implicarea consumatorului în procesul de elaborare, asamblare sau desfacere a bunurilor şi serviciilor pe care le achiziţionează, este, pe fond, o formă de exploatare[22] nedeclarată şi neconştientizată ca atare.

Aşadar, o primă utilitate a definirii muncii este tocmai conştientizarea celui care o prestează cu privire la faptul că activitatea sa este producătoare de valori, care probabil sunt monetizate de către un beneficiar ce exploatează fie caracterul plăcut, fie durata scurtă, fie componenta de notorietate pe care o prezintă, fie componenta ludică a muncii, cu scopul obţinerii unui profit.

O a doua utilitate priveşte identificarea muncii dependente. Este cu neputinţă să vorbim despre distincţia muncii dependente de munca independentă fără a stabili mai întâi care sunt graniţele muncii înseşi. Abia apoi vom putea aplica criteriile de identificare a unei munci subordonate, ce interesează dreptul muncii, de munca guvernată de contractele de drept civil. Şi menţionăm în treacăt că aceste criterii ar trebui, la rândul lor revizitate, deoarece schimbarea de paradigmă adusă cu sine de digitalizare a făcut ca multe dintre criteriile consacrate (dintre cele prevăzute, de exemplu, de Recomandarea Organizaţiei Internaţionale a Muncii, pe care o aminteam mai sus) să cadă în desuetudine.

În sfârşit, a identifica munca poate produce consecinţe şi în ceea ce priveşte delimitarea timpului de muncă de timpul de odihnă. Sub aspect juridic, perioada de repaus nu are o definiţie, fiind un concept rezidual: constituie timp de repaus tot ceea ce nu cade sub definiţia timpului de muncă. Este desigur firesc ca o normă juridică de drept al muncii să se preocupe de timpul de muncă, nu de timpul de repaus, şi să decurgă doar pe cale de consecinţă care ar putea constitui timpul de odihnă, prin scăderea din zi a timpului de muncă. Dar acest mod de normare produce anume consecinţe şi în plan psihologic, întreaga existenţă a persoanei active fiind centrată pe timpul de muncă.

8. Concluzii

Nu numai prestarea muncii este diferită în fiecare etapă istorică, nu numai profesiile se schimbă de la o generaţie la alta, nu numai percepţia socială asupra muncii este în continuă mobilitate, dar munca însăşi, adică activitatea pe care o valorizăm social ca fiind „muncă" – reprezintă un construct cultural, specific unui anumit moment şi unei anumite regiuni.

De-a lungul istoriei au existat o serie de momente cheie, care au modificat definiţia muncii: de la descoperirea agriculturii la influenţa religiei şi de la revoluţia industrială la războaiele mondiale. Trăim astăzi de asemenea un astfel de moment, prin digitalizarea muncii, care a adus cu sine noi valenţe ale muncii creative, o estompare a graniţei între muncă şi divertisment, dar şi moduri fără precedent de

[21] T. Terranova, *Network Culture: Politics for the Information Age*, London and Ann Arbor, MI: Pluto Press, 2004 p. 73.

[22] D. Zwick, S.K. Bonsu, A. Darmody, *op. cit.*, p. 177.

exploatare a activităţilor productive, prin deghizarea muncii în „non-muncă". Este vital aşadar să identificăm o serie de repere de natură să ne permită să o definim. Am socotit astfel că munca reprezintă o activitate învăţată ce presupune o alocare deliberată a energiei, care este orientată către un scop, se prestează în baza unui act juridic şi este solicitată de o altă persoană sau folositoare unei alte persoane decât lucrătorul însuşi.

Definirea muncii nu prezintă utilitate numai din punct de vedere social, psihologic sau antropologic, ci şi juridic. Ea face posibilă limitarea ipotezelor de exploatare a muncii, prin conştientizarea celui care o prestează cu privire la posibilitatea ca activitatea sa, deghizată adesea în divertisment, să fie de fapt muncă. Deşi conştientizarea nu pune capăt exploatării, ea constituie totuşi un prim pas în această direcţie. Definirea muncii este tot astfel utilă şi pentru demersul ce preocupă autorii de drept al muncii de astăzi, anume diferenţierea muncii subordonate de cea independentă. Şi este poate utilă şi pentru clarificarea limitelor (între care, cum arăta Curtea de Justiţie a Uniunii Europene, „nu există zonă gri") dintre timpul de muncă şi timpul de repaus.

Referinţe

Ali A.J., Al-Owaihan A., *Islamic work ethic: a critical review*, în Cross Cultural Management: An International Journal, Vol. 15 No. 1, 2008, pp. 5-19, https://doi.org/10.1108/13527600810848791

Anthony P. (ed.), *The Ideology of Work*, Tavistock Publications, 1977

Applebaum H., *The Concept of Work. Ancient, Medieval, and Modern*, State University of New York Press, 1992

Barbash J., Lampman R.J., Levitan S.A., Tyler G. (coord.), *The Work Ethic: A Critical Analysis,* Industrial Relations Research Association, Madison, WI, 1983

Cherrington D.J., *The Work Ethic: Working Values and Values That Work*, New York: Amacom, 1980

Dimitriu R., *Dreptul muncii. Anxietăţi ale prezentului*, Editura Rentrop şi Straton, Bucureşti, 2016

Glazer N., *Women's Paid and Unpaid Labor: The Work Transfer in Health Care and Retailing* (Women in the Political Economy), Philadelphia: Temple University Press, 1993

Hunnicutt B., *Work Is Our Religion And It's Failing Us*, Huffpost, 18 mai 2018

Iftichar A., *Islamic Labour Code*, Online

Ştefănescu I.T. (coord.), *Dicţionar de dreptul muncii*, Editura Universul juridic, Bucureşti, 2014

Suzman J., *Munca. O istorie a modului în care ne petrecem timpul* (traducere de Iulia Bertea-Nani), Editura Publica, 2021

Tabachiu A., *Psihologia muncii* (curs), Editura Universităţii Politehnice, Bucureşti, 1997

Terranova T., *Network Culture: Politics for the Information Age*, London and Ann Arbor, MI: Pluto Press, 2004

Zuboff S., *The Work Ethic and Organization*, în J. Barbash, R.J. Lampman, S.A. Levitan, G. Tyler (coord.), *The Work Ethic: A Critical Analysis,* Industrial Relations Research Association, Madison, WI, 1983

Zwick D., Bonsu S.K., Darmody A., *Putting Consumers to Work: 'Co-creation' and new marketing govern-mentality* în Journal of Consumer Culture, 2008; 8(2) pp. 163-196, https://doi.org/10.1177/1469540508090089

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-3

Unele consideraţii mai de aproape privind timpul de muncă la distanţă[1]

Some Considerations From a Closer Look at Distance Working Time

Septimiu Panainte[2]

Rezumat: Digitalizarea accentuată a activităţilor în ultimii ani a determinat creşterea semnificativă a situaţiilor în care munca este prestată de la distanţă. Dincolo de potenţialele avantaje, se pot identifica şi o serie de riscuri, iar printre acestea se află şi aspectele care privesc evidenţa şi gestionarea timpului de muncă. Legea nr. 81/2018 privind reglementarea activităţii de telemuncă poate fi apreciată ca adecvată în multe privinţe. Totuşi, conţine şi aspecte perfectibile privind: riscul stabilirii de condiţii restrictive în regulamentele interne în raport de stabilirea programului de lucru şi de verificarea activităţii telesalariaţilor de către reprezentanţii organizaţiilor sindicale ori de către reprezentanţii salariaţilor, reglementările concrete privind evidenţa timpului de lucru (sunt insuficiente), protecţia împotriva fragmentării excesive a timpului de lucru, necesitatea asigurării unui just echilibru între viaţa profesională şi cea privată a telesalariatului, consacrarea dreptul la deconectare etc.

Cuvinte-cheie: munca la distanţă; digitalizare; timp de muncă; program de muncă; dreptul la deconectare

Abstract: The increased digitalization of activities in recent years has induced to a significant evolution of situations in which work is performed remotely. Beyond the benefits, a number of risks can be identified, and among them are the aspects regarding the evidence and management of working time. Law no. 81/2018 on telework activity is definitely adequate in many aspects. But, also, it contains issues that can be improved regarding: the risk of setting up restrictive conditions in the internal regulations concerning the establishment of the work schedule or the verification of the activity of teleworkers by union representatives, concrete regulations on working time records, protection against excessive fragmentation of working time, the fair balance between the professional and

[1] Acest studiu a fost realizat în acord cu liniile directoare ale proiectului *Jean Monnet Module on EU Interdisciplinary Studies: Widening Knowledge for a more Resilient Union - EURES* (621262-EPP-1-2020-1-RO-EPPJMO) implementat de către Centrul de Studii Europene (Centru de excelenţă Jean Monnet) din cadrul Facultăţii de Drept, Universitatea „Alexandru Ioan Cuza” din Iaşi.

[2] Conferenţiar univ. dr., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iaşi, e-mail: septimiu.panainte@uaic.ro.

private life of the teleworker (is not enough taken into account), the right to disconnect (is not settled) etc.

Keywords: remote work; digitalization; working time; work schedule; right to disconnect

1. Aspecte introductive

Evoluţiile tehnologice şi digitalizarea accentuată a activităţilor în ultimii ani şi mai ales în perioada de pandemie au determinat dezvoltarea de forme din ce în ce mai eterogene de prestare a muncii, iar munca de la distanţă (în special telemunca, în sensul Legii nr. 81/2018 privind reglementarea activităţii de telemuncă[3]) este din ce în ce mai des întâlnită provocând şi atenţia doctrinei de specialitate[4].

Telemunca prezintă o serie de avantaje atât pentru salariat (reducerea sau eliminarea timpului de deplasare zilnic către locul de muncă, diminuarea riscului de îmbolnăvire în cazul bolilor contagioase, o mai mare autonomie şi flexibilitate în organizarea activităţii, o mai mare productivitate, posibilităţi mai mari de adaptare a activităţii profesionale la viaţa de familie etc.), cât şi pentru angajator (acesta poate beneficia de o posibilă creştere a motivaţiei salariaţilor şi de o eficienţă mai ridicată a muncii, de reducerea sau eliminarea completă a unor costuri etc.). Aceste avantaje sunt în marea lor majoritate potenţiale şi pot deveni realitate dacă sunt favorizate de reglementări adecvate şi de o abordare constructivă a părţilor la raporturile juridice de muncă (depind în mare măsură în special de

[3] Publicată în M.Of. nr. 296 din 02 aprilie 2018. Prezentul studiu nu are în vedere munca la domiciliu, ca formă a muncii la distanță, în reglementarea acesteia prin dispozițiile art. 108-110 din Codul muncii.

[4] A se vedea, spre exemplu, M.-E. Marica, *Contracte de muncă atipice*, Editura Universul juridic, Bucureşti, 2019; A. Ștefănescu, *Munca la domiciliu şi telemunca. Drept intern şi comparat*, Editura Universul Juridic, Bucureşti, 2011; A, Cioriciu Ștefănescu, *Telemunca*, în R.R.D.M., nr. 1/2009, pp. 60-105; C.-A. Moarcăș, *Efectele globalizării, transformarea relației de muncă și regândirea dialogului social*, în RRDP, nr. 4/2019, *Autonomia dreptului muncii*, coordonatori A. Athanasiu, L. Dima, pp. 55-79; L. Dima, *Aspecte de noutate privind mijloacele materiale de probă în contextul noilor tehnologii*, în *Conferința Internațională de Dreptul Muncii - Noile tehnologii, consecințe asupra raportului de muncă*, Sibiu, 11-12 octombrie 2019, Editura Universul Juridic, 2020, pp. 59-70; M. Gheorghe, *Munca prestată prin utilizarea platformelor digitale. Consecințe asupra principiului egalității de tratament*, în *Conferința Internațională de Dreptul Muncii - Noile tehnologii..., cit. supra,* pp. 166-171; C.C. Nenu, *Evoluția conceptului de securitate și sănătate în muncă în contextul noilor tehnologii*, în *Conferința Internațională de Dreptul Muncii Noile tehnologii..., cit. supra,* pp. 118-123; S. Panainte, *Considerații privind alienarea salariatului în industria 4.0.*, în *Conferința Internațională de Dreptul Muncii - Noile tehnologii..., cit. supra,* pp. 172-181; J.-M. Servais, *Economia colaborativă a platformelor electronice: noi provocări, noi protecții*, în *Conferința Internațională de Dreptul Muncii - Noile tehnologii..., cit. supra,* pp. 11-33; M. Țichindelean, *Considerații privind protecția datelor cu caracter personal în raporturile de muncă prin utilizarea mijloacelor de supraveghere video*, în *Conferința Internațională de Dreptul Muncii - Noile tehnologii..., cit. supra*, pp. 83-89.

specificul activităţii şi de nivelul de elevare a managementului resurselor umane aplicat în practică).

În acelaşi timp însă, nu trebuie neglijate riscurile pe care le induce munca la distanţă în două planuri majore şi definitorii pentru relaţia de muncă: cel al sănătăţii şi securităţii în muncă şi cel al echilibrului dintre viaţa profesională şi viaţa privată a lucrătorului. Aceste riscuri sunt sublimate în practică prin predispoziţia la program prelungit şi efectuarea de ore suplimentare, creşterea sau diluarea intensităţii muncii, fragmentarea excesivă a programului de lucru, invadarea spaţiului privat prin activităţi de monitorizare a activităţii, expunerea unor date cu caracter personal, izolarea şi creşterea nivelului de stres profesional şi de oboseală, expunerea excesivă la radiaţiile de radiofrecvenţă, perceperea activităţii efectuate de la distanţă ca periferică şi riscul producerii unor acte de discriminare în special indirectă a telesalariaţilor, comparativ cu cei care desfăşoară activităţi la locurile de muncă organizate de către angajator în cadrul structurilor acestuia, dificultăţi de sindicalizare etc. În mod evident, în cazul decuplării activităţii salariatului de locul de muncă tradiţional şi plasării acesteia în special la domiciliu este amplificat riscul unei suprapuneri sau, după caz, unei interferenţe mai acute între viaţa profesională şi cea privată, aspect care reclamă metode adecvate de echilibrare.[5] Dintr-o altă perspectivă, munca la distanţă are potenţialul de a favoriza creşterea activităţilor pe bază de contracte cu elemente particulare sau chiar atipice, cum ar fi cele *on call* sau *zero hours,* cu toate vulnerabilităţile pe care acestea le presupun.

Pe acest fond, adoptarea Legii nr. 81/2018 privind reglementarea activităţii de telemuncă a semnificat asumarea de către legiuitor a scopului protectiv în raport de aspectele specifice telemuncii[6], în mod special în planul sănătăţii şi securităţii în muncă a salariaţilor.

2. Aspecte generale privind timpul de muncă la distanţă

Aspectele privind timpul de muncă sunt în mod esenţial subsumate asigurării sănătăţii şi securităţii în muncă a salariaţilor, iar reglementarea timpului de muncă are foarte adesea ca scop principal sau secundar garantarea timpului de repaus necesar pentru refacerea capacităţii de muncă. De altfel, prin art. 1 alin. (1) din Directiva 2003/88/CE privind anumite aspecte ale organizării timpului de lucru

[5] Pentru detalii, a se vedea Raportul OIM, *Ensuring decent working time for the future*, International Labour Conference, 107th Session, 2018, *General Survey concerning working-time instruments*, Geneva, 2018, Report of the Committee of Experts on the Application of Conventions and Recommendations (articles 19, 22 and 35 of the Constitution), Report III (Part B), [Online] la https://www.ilo.org/ilc/ILCSessions/previous-sessions/107/reports/reports-to-the-conference/WCMS_618485/lang--en/index.htm, accesat 29.09.2021.

[6] Conform art. 2 lit. a, în sensul Legii nr. 81/2018, prin „telemuncă" se înţelege acea „formă de organizare a muncii prin care salariatul, în mod regulat şi voluntar, îşi îndeplineşte atribuţiile specifice funcţiei, ocupaţiei sau meseriei pe care o deţine în alt loc decât locul de muncă organizat de angajator, folosind tehnologia informaţiei şi comunicaţiilor".

este stabilit că aceasta „stabileşte cerinţe minime de securitate şi sănătate pentru organizarea timpului de lucru". Directiva nu reglementează expres aspecte privind timpul de muncă la distanţă.

Deşi adeseori criticată pentru caracterul incomplet sau nenuanţat al reglementării (din perspectiva abordării binare – timp de lucru şi de repaus), directiva a constituit un cadru referenţial pentru dezvoltarea unei jurisprudenţe bogate a CJUE care a dat consistenţă standardului de protecţie minimal necesar a fi avut în vedere de statele membre[7].

Suplimentar, timpul de lucru şi de repaus trebuie privit prin prisma necesităţii asigurării unui just echilibru între viaţa profesională şi cea privată a telesalariatului. Dreptul intern nu tratează expres şi direct această perspectivă, iar reglementările dreptului european sunt limitate la acest moment la Directiva 2019/1158 privind echilibrul dintre viaţa profesională şi cea privată a părinţilor şi îngrijitorilor şi de abrogare a Directivei 2010/18/UE a Consiliului[8].

În privinţa muncii la distanţă, aceasta a fost avută în vedere la adoptarea Directivei 2019/1152 privind transparenţa şi previzibilitatea condiţiilor de muncă în Uniunea Europeană[9]. Este aşteptată cu deosebit interes adoptarea directivei privind dreptul lucrătorilor de a se deconecta[10].

În planul dreptului intern, reglementarea generală privind timpul de muncă şi timpul de odihnă este constituită de art. 111 – 158 din Codul muncii, aplicabilă şi telemuncii în lipsa unor dispoziţii speciale derogatorii în Legea nr. 81/2018.

Timpul de muncă şi, implicit de repaus, este organic legat de alte elemente cum ar fi organizarea muncii, normarea muncii[11], programul de lucru, evidenţa orelor lucrate ş.a.[12]

Impunerea acordului scris al telesalariatului cu normă întreagă pentru prestarea de muncă suplimentară este binevenită (art. 4 alin. (2) din Legea nr. 81/2018). Trebuie să înţelegem că este vorba de acordul prealabil şi special, vizând anumite ore suplimentare, clar individualizate. În lipsa unei dispoziţii derogatorii,

[7] De-a lungul timpului, CJUE a fost chemată să interpreteze prevederile directivei mai ales în considerarea unor situații particulare. Aspectele statuate de către Curte, inclusiv în unele cauze recent soluționate, în special cu privire la delimitarea timp de muncă/timp de odihnă, sunt de natură să sublinieze necesitatea unor noi soluții de reglementare în acord cu o realitate economică și socială care a devenit deosebit de eterogenă și se află în proces de schimbare accelerată.

[8] Publicată în JO L 188, 12.7.2019, p. 79–93.

[9] Publicată în JO L 186, 11.7.2019, p. 105–121.

[10] A se vedea Rezoluția Parlamentului European din 21 ianuarie 2021 conținând recomandări adresate Comisiei privind dreptul de a se deconecta (2019/2181(INL)), [Online] la https://www.europarl.europa.eu/doceo/document/TA-9-2021-0021_ RO.html, accesat 29.09.2021.

[11] În alegerea legiuitorului român, norma de muncă este reglementată de Codul muncii în secțiune distinctă din cadrul capitolului dedicat timpului de muncă.

[12] Directiva 89/391 privind punerea în aplicare de măsuri pentru promovarea îmbunătățirii securității și sănătății lucrătorilor la locul de muncă (Directiva-cadru europeană privind securitatea și sănătatea în muncă).

contractul cu timp parţial şi muncă la distanţă este posibil, în acest caz prestarea orelor suplimentare fiind interzisă ca urmare a aplicării regulii generale prevăzute de art. 105 alin. (1) lit. c) din Codul muncii.

O altă deosebire faţă de regimul comun al raporturilor de muncă priveşte faptul că, în cazul telemuncii, programul de lucru este organizat prin acordul părţilor, cu respectarea contextului normativ şi convenţional (art. 4 alin. (1) din Legea nr. 81/2018). În acest mod, în principiu, programul de lucru poate fi adaptat, inclusiv în privinţa fragmentării acestuia, la necesităţile şi dorinţele salariaţilor care ţin de viaţa privată a acestora.

Conform art. 5 alin. (2) lit. d) şi e) din Legea nr. 81/2018, în cazul activităţii de telemuncă trebuie avute în vedere, suplimentar faţă de elementele de conţinut ale obligaţiei de informare prevăzute la art. 17 alin. (3) din Codul muncii: programul în cadrul căruia angajatorul este în drept să verifice activitatea telesalariatului şi modalitatea concretă de realizare a controlului; modalitatea de evidenţiere a orelor de muncă prestate de telesalariat. Aceste elemente specifice au dimensiune convenţională şi trebuie să se regăsească şi în conţinutul înscrisului contractual/actului adiţional, după caz.

Faţă de cele de mai sus, considerăm că, pentru rigoare, şi programul de lucru trebuia inclus printre elementele de conţinut ale obligaţiei de informare specifice telemuncii.

3. Observaţii şi aprecieri critice privind reglementarea timpului de muncă la distanţă

3.1. Atât timp cât munca este desfăşurată de la distanţă prin utilizarea tehnologiilor de comunicare moderne, acestea asigurând mobilitatea lucrătorului, interesul angajatorului pentru a solicita prestarea activităţii într-un anumit loc (oricum în afara perimetrului organizat de către acesta) este minimal, uneori fiind chiar contraindicat acest lucru. Cel mai adesea, având în vedere potenţialele avantaje pentru îmbunătăţirea echilibrului între viaţa profesională şi cea privată a telesalariatului, dar şi restricţiile impuse pe fond pandemic, activitatea se desfăşoară de la domiciliul acestuia (în sens larg)[13].

[13] Art. 5 alin. (2) lit. c) din Legea nr. 81/2018, privind menționarea în contractul de muncă a locului sau locurilor din care se desfășoară activitatea de telemuncă, a fost abrogat prin art. II pct. 3 din OUG nr. 36/2021 privind utilizarea semnăturii electronice în domeniul relațiilor de muncă și pentru modificarea și completarea unor acte normative, publicată în M.Of. nr. 474 din 06.05.2021, aprobată cu modificări și completări prin Legea nr. 208/2021. Resortul acestei abrogări ar putea fi acela că textul era de prisos în condițiile în care art. 17 alin. (3) lit. b) coroborat cu alin. (4) din Codul muncii prevede oricum obligația de informare și menționarea în contractul de muncă a locului de muncă sau, în lipsa unui loc de muncă fix, a posibilității ca salariatul să muncească în diverse locuri. Având în vedere specificul telemuncii, abrogarea ar putea avea ca semnificație și faptul că locul concret al muncii de la distanță nu este, ca regulă, determinant din perspectiva formării și scopului contractului, putând fi lăsat chiar la latitudinea salariatului (în mod evident însă, din perspectiva îndeplinirii obligațiilor specifice privind sănătatea și securitatea în muncă de către

3.2. Reţinând acest aspect, devine evident că programul de lucru capătă o importanţă deosebită. De altfel, acest aspect poate fi sesizat şi din prioritatea în reglementare (art. 4 din lege). Se impun o serie de observaţii.

În primul rând, în formularea art. 4 alin. (1) din lege, „telesalariaţii organizează programul de lucru de comun acord cu angajatorul". Considerăm că în mod corect legiuitorul nu a apelat la soluţia corespondentă consacrată de Codul muncii în cazul contractului cu munca la domiciliu[14]. Din perspectiva reglementării, cele două forme de muncă la distanţă presupun premise sensibil diferite.

În sensul Acordului-cadru european privind telemunca din 2002[15], telesalariaţii îşi pot gestiona singuri timpul de muncă, cu respectarea dispoziţiilor legale, contractelor colective de muncă şi regulilor adoptate la nivelul angajatorilor (pct. 9). Această opţiune are ca efect direct maximum de flexibilitate, iar indirect, probabil, un mai bun echilibru între viaţa privată şi cea profesională a telesalariaţilor, dar şi riscul desubstanţializării unor norme protective pentru salariat.

O atare opţiune de reglementare presupune în mod necesar şi responsabilizarea salariaţilor printr-o serie de reguli complementare. Ca premisă, din moment ce angajatorul nu are control asupra deciziei telesalariatului de organizare a timpului de muncă, nici nu va putea fi obligat suplimentar ca urmare a deciziei unilaterale a cocontractantului. Pe cale de consecinţă, „preţul" pentru a beneficia de maximum de flexibilitate poate fi faptul că telesalariaţii nu ar putea solicita plata de sporuri pentru ore suplimentare, muncă de noapte sau in perioadele de repaus (sens în care au fost date ca exemplu reglementările din Cehia şi Slovacia), sau, în general, de nici un fel de beneficiu suplimentar de timp liber sau financiar care ar putea rezulta din prestarea muncii în afara programului

angajator și al verificărilor posibile, inclusiv și mai ales când este la domiciliul salariatului, locul muncii este relevant). Și Directiva (UE) 2019/1152 privind transparența și previzibilitatea condițiilor de muncă în Uniunea Europeană prevede printre elementele care fac obiectul obligației de informare „locul de desfășurare a activității; dacă nu există un loc de desfășurare a activității fix sau principal, principiul conform căruia lucrătorul are diverse locuri de desfășurare a activității sau este liber să își stabilească propriul loc de desfășurare a activității" (art. 4 alin. (2) lit. b).

[14] Art. 108 alin. (2) din Codul muncii: „În vederea îndeplinirii sarcinilor de serviciu ce le revin, salariații cu munca la domiciliu își stabilesc singuri programul de lucru". Pentru telemuncă această soluție ar fi fost nerealistă, mai ales în condițiile actuale. Spre deosebire, legiuitorul a dovedit consecvență din perspectiva impunerii ca programul în cadrul căruia angajatorul este în drept să verifice activitatea salariatului și modalitatea concretă de realizare a controlului să facă obiectul acordului de voință a părților și să fie menționate în contract (art. 109 lit. b) din Codul muncii, art. 5 alin. (2) lit. d) din Legea nr. 81/2018).

[15] [Online] la https://resourcecentre.etuc.org/sites/default/files/2020-09/Telework%202002_Framework%20 Agreement%20-%20EN.pdf, accesat 29.09.2021.

normal de muncă (în acest sens fiind dat ca exemplu contractul colectiv pentru sectorul serviciilor financiare din Danemarca)[16].

Revenind la soluţia consacrată de legea română, din moment ce angajatorul îşi exprimă acordul cu privire la modul de organizare a programului de lucru propus de telesalariat, îşi asumă şi toate consecinţele juridice pentru situaţii de tipul celor expuse mai sus. În acest fel, normele protective în materie de timp de muncă şi de repaus îşi pot atinge finalitatea.

În al doilea rând, remarcăm faptul că Legea nr. 81/2018 nu impune expres ca acordul părţilor în privinţa programului de lucru să aibă formă scrisă. Această condiţie privind forma nu poate fi dedusă nici din faptul că acest acord trebuie realizat „în conformitate cu prevederile contractului individual de muncă, regulamentului intern şi/sau contractului colectiv de muncă aplicabil, în condiţiile legii". Considerăm că această soluţie de reglementare este de natură să faciliteze o oarecare variabilitate sau volatilitate a programului de lucru şi să conducă la probleme în planul capacităţii de a se dovedi anumite aspecte, fie în faţa inspectorilor de muncă, fie în faţa instanţei de judecată. Chiar dacă angajatorul trebuie să îşi îndeplinească obligaţia de a ţine evidenţa muncii prestate în modalitatea agreată cu telesalariatul, considerăm că se diminuează efectul pozitiv al impunerii formei scrise a acordului pentru efectuarea orelor suplimentare. Totodată, lipsa unui înscris probator pentru programul de lucru poate genera probleme şi în alte planuri: din perspectiva calificării muncii de noapte sau necesităţii verificării respectării timpului de repaus exprimat în ore consecutive; în cercetarea disciplinară, spre exemplu când se analizează eventuale absenţe nemotivate de la program etc. Mai apreciem că numai dacă programul de lucru este cunoscut în mod exact, fiind susceptibil de a fi comunicat doar de o parte a contractului, reprezentanţii organizaţiilor sindicale la nivel de unitate ori reprezentanţii salariaţilor sau inspectorii de muncă vor putea proceda în mod eficient la verificările instituite în competenţa lor conform art. 9 din lege.

Aşadar, punând în balanţă avantajul flexibilităţii şi riscurile de mai sus, apreciem că se impune completarea art. 4 din lege în sensul impunerii acordului în formă scrisă[17].

În al treilea rând, observăm că acordul părţilor privind organizarea programului de lucru se poate realiza „în conformitate cu prevederile contractului individual de muncă, regulamentului intern şi/sau contractului colectiv de muncă aplicabil, în condiţiile legii". Această enumerare, de altfel recurentă în cuprinsul

[16] A se vedea Raportul Eurofound *Telework in the European Union*, publicat la 10.01.2010, [Online] la https://www.eurofound.europa.eu/bg/publications/report/2010/telework-in-the-european-union, p. 17, accesat 29.09.2021.

[17] La par. 31 din preambulul Directivei (UE) 2019/1152 privind transparența și previzibilitatea condițiilor de muncă în UE se menționează: „Orele și zilele de referință, care se interpretează ca fiind intervalele orare în care poate fi prestată munca la solicitarea angajatorului, ar trebui să fie stabilite în scris la începutul raportului de muncă". Și o eventuală reglementare a dreptului la deconectare este condiționată de certitudinea programului de lucru și de posibilitățile salariatului de a îl dovedi în caz de conflict.

Legii nr. 81/2018, priveşte premisele şi limitele în care părţile îşi pot exprima voinţa şi este criticabilă.

Astfel, alăturarea celor trei categorii de acte, diferite prin modul de formare şi scopuri, precum şi ordinea enumerării acestora, par mai degrabă aleatorii.

Contractul individual de muncă exprimă voinţa părţilor, în condiţiile legii şi ţinând cont de prevederile contractului colectiv de muncă, întocmai ca şi acordul privind programul de lucru. Dincolo de potenţiala asimetrie de formă, un acord ulterior încheierii contractului individual poate modifica şi modifică acel contract şi nu poate fi ţinut de prevederile iniţiale care eventual se intenţionează a fi modificate. Reglementarea se poate justifica într-o oarecare măsură în situaţia în care contractul individual nu prevede anumite aspecte şi se impune a fi completat ţinându-se cont de anumite repere determinante sau circumstanţiale conţinute în înscrisul contractual. *E.g.,* stabilirea programului de lucru trebuie convenită în raport de felul muncii prevăzut în contract şi, eventual, de poziţia executivă sau managerială în structura organizaţională a angajatorului. Această interpretare fundamentată pe raţionamentul determinării limitelor în care se poate stabili programul de lucru prin alte elemente extrinseci acestuia ar putea fi primită şi cu privire la referirea la contractul colectiv de muncă.

Mai greu asimilabilă este însă trimiterea la regulamentul intern. Acesta este adoptat de către angajator, doar în baza consultării sindicatului sau a reprezentanţilor salariaţilor, după caz, şi nu în baza acordului acestora (art. 241 din Codul muncii). Aşadar, există riscul stipulării unilaterale în regulamentul intern a unor condiţii legale, dar restrictive în privinţa programului de lucru, aspect care poate conduce la limitarea libertăţii de voinţă a telesalariatului de către angajator.

Enumerarea analizată mai apare criticabilă prin prisma faptului că, pentru situaţia unui concurs, nu prioritizează în privinţa izvoarelor condiţiilor în care se poate stabili programul de lucru prin acordul părţilor. Din această perspectivă, pentru situaţia în care aceste condiţii ar fi tratate simultan diferit în surse distincte, s-ar putea urma soluţia de reglementare oferită de art. 63 alin. (2) din Codul muncii (prin care se acordă prioritate contractului colectiv de muncă în faţa regulamentului intern).

În al patrulea rând, Legea nr. 81/2018 nu conferă expres programului de lucru relevanţă în contextul reglementării verificărilor care pot interveni în cazul telemuncii, respectiv:

a) *verificarea activităţii telesalariatului de către angajator.* Conform art. 5 alin. (2) lit. d) din Legea nr. 81/2018, programul în cadrul căruia angajatorul este în drept să verifice activitatea telesalariatului şi modalitatea concretă de realizare a controlului trebuie să se regăsească în înscrisul contractual sau act adiţional; verificarea activităţii se realizează „în principal prin utilizarea tehnologiei informaţiei şi comunicaţiilor, în condiţiile stabilite prin contractul individual de

muncă, regulamentul intern şi/sau contractul colectiv de muncă aplicabil, în condiţiile legii" (art. 4 alin. (3) din Legea nr. 81/2018).[18]

b) *verificarea condiţiilor de muncă ale telesalariatului de către reprezentanţii organizaţiilor sindicale la nivel de unitate ori reprezentanţii salariaţilor.* În temeiul alin. (1) al art. 9 din Legea nr. 81/2018, pentru aplicarea şi verificarea condiţiilor de muncă ale telesalariatului, reprezentanţii organizaţiilor sindicale la nivel de unitate ori reprezentanţii salariaţilor au acces la locurile de desfăşurare a activităţii de telemuncă, „în condiţiile stipulate în contractul colectiv de muncă sau contractul individual de muncă ori regulamentul intern, după caz"[19].

c) *verificarea aplicării şi respectării cerinţelor legale din domeniul securităţii şi sănătăţii în muncă şi al relaţiilor de muncă de către reprezentanţii autorităţilor competente*: conform alin. (2) al art. 9, pentru a realiza activităţile de control reprezentanţii autorităţilor au dreptul de acces la locurile de desfăşurare a activităţii de telemuncă, în condiţiile stipulate în Legea nr. 108/1999 pentru înfiinţarea şi organizarea Inspecţiei Muncii.

Doar pentru ipoteza în care locul de desfăşurare a activităţii telesalariatului este la domiciliul acestuia (în sens larg), dreptul de acces pentru verificarea condiţiilor de muncă, respectiv respectării cerinţelor legale din domeniul securităţii şi sănătăţii în muncă, este condiţionat de notificarea prealabilă a telesalariatului şi de exprimarea consimţământului acestuia (art. 9 alin. 3)[20]. Pentru accesul în domiciliu, acordul salariatului trebuie să fie prealabil şi special. Prin urmare, în acest caz, nu se poate vorbi de o verificare inopinată cu scop de surprindere a realităţii respectării de către salariat a condiţiilor de desfăşurare a activităţii.

După cum am arătat, programul în cadrul căruia angajatorul este în drept să verifice activitatea telesalariatului şi modalitatea concretă de realizare a controlului trebuie prevăzute în contractul de muncă sau în act adiţional la acesta. Pentru situaţia în care activitatea se desfăşoară la domiciliul salariatului Legea nr. 81/2018 nu impune expres consimţământul expres şi prealabil al acestuia, raportat la fiecare act de control, oricare ar fi modalitatea de verificare agreată de părţi. Premisa de la care a plecat legiuitorul a fost cea enunţată în art. 4 alin. 3 din lege, respectiv că verificarea activităţii se realizează „în principal prin utilizarea tehnologiei informaţiei şi comunicaţiilor", deci tot de la distanţă, fără a fi nevoie de verificare fizică sau detaliată în spaţiul în care salariatul prestează munca. Totuşi nu este exclus ca asemenea verificări să fie necesare şi convenite de părţi. Dacă munca este

[18] Și cu privire la acest aspect se poate reține riscul subliniat mai sus ca prin regulamentul intern să fie impuse limite ale exprimării voinței salariatului.

[19] Regăsim aceeași disonanță: reprezentanții organizațiilor sindicale la nivel de unitate ori reprezentanții salariaților pot exercita un drept în condițiile stipulate în regulamentul intern adoptat de către angajator. Or, prin verificarea condițiilor de muncă ale telesalariatului, reprezentanții sindicatului sau salariaților verifică și dacă angajatorul și-a îndeplinit obligațiile aferente, nu numai dacă salariatul le respectă.

[20] Consimțământul salariatului este, fără îndoială, important prin prisma protecției dreptului la respectarea vieții private și de familie (în sensul art. 8 din CEDO și art. 26 și 27 din Constituția României).

prestată de la domiciliul salariatului şi pentru verificările care revin autorităţilor statului se impune acordul expres al acestuia, cu atât mai mult acest acord este necesar în cazul verificărilor efectuate de către angajator. Altfel, ar exista riscul subordonării aspectelor care ţin de viaţa privată a salariatului şi membrilor familiei acestuia faţă de activitatea profesională – verificările domiciliare întreprinse de către angajator.

Mai avem în vedere faptul că activităţile de control presupun, în principiu, prezenţa sau cel puţin disponibilitatea de la distanţă a salariatului. Pe cale de consecinţă, în lumina jurisprudenţei CJUE[21], intervalul în care se realizează sau se poate realiza controlul constituie perioadă în care salariatul, chiar dacă nu ar presta în mod efectiv activitate, se află într-o formă de exercitare a funcţiei sale şi, drept urmare, acest interval trebuie calificat ca fiind timp de muncă în sensul art. 2 pct. 1 din Directiva 88/2003.

Aşadar, dacă munca este prestată de la domiciliu, apreciem că, pentru a nu fi intruzive, toate activităţile de control sunt condiţionate de exprimarea consimţământului salariatului[22] şi trebuie realizate în timpul programului de lucru. Pentru ipoteza în care activitatea nu se desfăşoară de la domiciliu, ci în alt loc agreat de părţi sau lăsat la alegerea telesalariatului, apreciem că acestea trebuie realizate, de asemenea, în timpul şi cu respectarea programului de lucru.

3.3. Un alt aspect specific muncii la distanţă, care este de natură să ridice probleme de ordin practic, este cel privind evidenţa orelor de muncă prestate zilnic de către telesalariat.

La nivel general, CJUE a statuat în cauza C-55/18 că normele europene impun statelor naţionale obligaţia de a impune angajatorilor instituirea unui sistem care să permită măsurarea duratei timpului de lucru zilnic efectuat de fiecare lucrător[23].

---

[21] A se vedea, spre exemplu, cauza *Ville de Nivelles vs. Rudy Matzak* (C-518/15), par. 59 şi jurisprudenţa citată.

[22] În acest sens este şi pct. 8 din Acordul cadru european privind telemunca din 2002 (*The European Framework Agreement on Telework*) care se referă la notificarea prealabilă şi la necesitatea consimțământului telesalariatului care prestează activități de la domiciliu pentru verificările efectuate de angajator, reprezentanții salariaților sau autoritățile competente în privința sănătății și securității în muncă (în măsura în care presupun accesul în domiciliu).

[23] Hotărârea CJUE (Marea Cameră) din 14 mai 2019, în cauza C-55/18, *Federación de Servicios de Comisiones Obreras (CCOO) v. Deutsche Bank SAE*: „Articolele 3, 5 și 6 din Directiva 2003/88/CE a Parlamentului European și a Consiliului din 4 noiembrie 2003 privind anumite aspecte ale organizării timpului de lucru, citite în lumina articolului 31 alineatul (2) din Carta drepturilor fundamentale a Uniunii Europene, precum și a articolului 4 alineatul (1), a articolului 11 alineatul (3) și a articolului 16 alineatul (3) din Directiva 89/391/CEE a Consiliului din 12 iunie 1989 privind punerea în aplicare de măsuri pentru promovarea îmbunătățirii securității și sănătății lucrătorilor la locul de muncă, trebuie interpretate în sensul că se opun unei reglementări a unui stat membru care, potrivit interpretării care este dată acesteia de către jurisprudența națională, nu impune angajatorilor obligația de a institui un sistem care să permită măsurarea duratei timpului de lucru zilnic efectuat de fiecare lucrător”.

Codul muncii a reglementat încă din forma iniţială obligaţia angajatorilor de a ţine evidenta orelor de muncă prestate de fiecare salariat. În prezent, art. 119 din Cod prevede la alin. (1) obligaţia angajatorului „de a ţine la locul de muncă definit potrivit art. 16[1] evidenţa orelor de muncă prestate zilnic de fiecare salariat, cu evidenţierea orelor de începere şi de sfârşit ale programului de lucru, şi de a supune controlului inspectorilor de muncă această evidenţă, ori de câte ori se solicită acest lucru". Aşadar, ca regulă generală, îndatorirea de a ţine evidenţa activităţilor prestate revine angajatorului, acesta putând stabili în mod unilateral modalitatea concretă în care îşi îndeplineşte obligaţia.

Al doilea alineat al art. 119 tratează situaţia particulară a trei categorii de salariaţi (mobili, care desfăşoară muncă la domiciliu şi din cadrul microîntreprinderilor); pentru aceştia „angajatorul ţine evidenţa orelor de muncă prestate zilnic de fiecare salariat în condiţiile stabilite cu salariaţii prin acord scris, în funcţie de activitatea specifică desfăşurată de către aceştia". La aceste categorii putem adăuga şi telesalariaţii, Legea nr. 81/2018 prevăzând la art. 5 alin. (2) lit. e) faptul că modalitatea de evidenţiere a orelor de muncă prestate de telesalariat trebuie să se regăsească în conţinutul contractului individual de muncă (deci are natură convenţională şi presupune exprimarea voinţei părţilor în scris). Raportat la aceste patru categorii de salariaţi, faptul că modalităţile şi condiţiile concrete de evidenţiere a muncii presupun acceptul acestora, nu semnifică faptul că obligaţia de a ţine evidenţa muncii nu rămâne exclusiv în sarcina angajatorului. Pentru a îşi îndeplini obligaţia, angajatorul va trebui să găsească o formula de evidenţiere adecvată, acceptabilă şi acceptată de salariaţii respectivi.

Dimensiunea convenţională a modalităţilor concrete de evidenţiere în cazul telesalariaţilor poate fi justificată prin necesitatea ca acestea să fie cunoscute de către aceştia, să fie adecvate naturii şi specificului activităţii şi prin perspectiva invocării în faţa organelor de control sau în faţa instanţelor de judecată a unor probe în consecinţă: înscrisuri (eventual electronice), mijloace materiale de probă etc.

În mod evident, în multe situaţii utilizarea tradiţionalei condici de prezenţă nu mai apare ca o soluţie viabilă. În cazul telesalariaţilor apare a fi adecvată şi, în consecinţă, mai probabilă, utilizarea unor aplicaţii informatice dedicate înregistrării timpului în care se prestează activitatea. Având în vedere că programele software utilizate pot avea funcţii complexe, trebuie delimitat între funcţia de contabilizare a timpului de muncă şi cea de monitorizare sau verificare a activităţii efectiv prestată de telesalariat[24]. Am arătat deja că şi modalitatea concretă de

[24] Pentru unele detalii a se vedea M. Samek Lodovici *et al., The impact of teleworking and digital work on workers and society. Special focus on surveillance and monitoring, as well as on mental health of workers*, 2021, publication for the Committee on Employment and Social Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, [Online] la https://op.europa.eu/en/publication-detail/-/publication/49c693a2-cfdb-11eb-ac72-01aa75ed71a1/language-en, accesat 29.09.2021, şi [Online] la http://www.europarl.europa.eu/supporting-analyses.

realizare a controlului activităţii presupune acordul telesalariatului (art. 5 alin. (2) lit. d), independent de faptul că acesta lucrează de la domiciliu sau nu.

Mai trebuie adăugat că în cazul în care angajatorul intenţionează utilizarea unor sisteme de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video la locul de muncă[25] art. 5 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)[26] impune măsuri deosebit de stricte pentru prelucrarea datelor cu caracter personal ale salariaţilor. Astfel, dacă sunt utilizate asemenea sisteme de monitorizare, prelucrarea acestor date se poate realiza exclusiv în scopul realizării intereselor legitime urmărite de angajator şi este permisă numai dacă:

„a) interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate;

b) angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor;

c) angajatorul a consultat sindicatul sau, după caz, reprezentanţii angajaţilor înainte de introducerea sistemelor de monitorizare;

d) alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienţa; şi

e) durata de stocare a datelor cu caracter personal este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate".

Faţă de caracterul imperativ al normei expuse, la nivel general, apreciem că, independent de locul desfăşurării activităţii, aceste condiţii nu sunt „negociabile" între salariaţi şi angajatori în considerarea dreptului persoanelor fizice de a dispune în privinţa datelor lor cu caracter personal. Se poate invoca, suplimentar, contextul executării contractului de muncă şi incidenţa art. 38 din Codul muncii.

Protecţia datelor cu caracter personal este însă cu atât mai necesară în condiţiile în care munca este îndeplinită de la distanţă şi mai ales când este prestată de la domiciliul telesalariatului folosind tehnologia informaţiei şi comunicaţiilor. În acest context, considerăm că acordul telesalariatului privind verificarea activităţii sale prin asemenea sisteme de monitorizare poate fi solicitat de către angajator numai după ce acesta s-a asigurat că sunt îndeplinite condiţiile impuse de art. 5 din Legea nr. 190/2018, citate mai sus. Aşadar, acordul salariatului în privinţa utilizării acestor sisteme nu poate implica şi nu se poate interpreta şi în sensul degrevării angajatorului de sarcina îndeplinirii condiţiilor impuse de lege.

[25] A se vedea și Hotărârea CtEDO nr. 61496/08 din septembrie 2017, în cauza Bărbulescu contra României, [Online] la https://hudoc.echr.coe.int/eng#{%22tabview%22: [%22 document%22],%22itemid %22:[%22001-180112%22]}.

[26] Publicată în M.Of. 651 din 26.07.2018.

Dacă angajatorul, verificând condiţia ca alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator să nu îşi fi dovedit anterior eficienţa, nu are o altă alternativă în afara celei propuse telesalariatului şi acesta nu o acceptă, se va putea deduce că munca la distanţă nu este posibilă.

3.4. Organizarea programului de lucru la distanţă de către părţi de comun acord (art. 4 alin. (1)) prezintă potenţialul avantaj de a se agrea formule flexibile de lucru, reciproc avantajoase. Pe de altă parte, în condiţiile în care programul de lucru este subsumat în principal necesităţilor angajatorului şi/sau excesiv fragmentat, trebuie considerat riscul unor potenţiale efecte negative asupra echilibrului necesar între viaţa privată şi cea profesională a telesalariatului.

În acest context trebuie subliniat standardul minimal impus de Codul muncii în materie de repaus: cel puţin 12 ore consecutive între două zile de muncă (art. 135 alin. (1)) şi 48 de ore consecutive de repaus săptămânal, de regulă sâmbăta şi duminica (art. 137 alin. (1))[27].

În perspectivă, nu trebuie exclus ca şi durata maximă a timpului zilnic de lucru să fie reevaluată şi, eventual, redusă, având în vedere riscurile inerente pentru sănătatea salariaţilor pe care le atrage activitatea prelungită care presupune utilizarea computerelor.

3.5. Mai poate fi subliniat faptul că munca de la distanţă este de natură să conducă la creşterea raporturilor de muncă cu elemente de extraneitate[28]. Faţă de obiectul prezentului studiu, relevăm riscul gestionării cu dificultate a programului de lucru raportat la fusul orar la care se raportează telesalariaţii, angajatorii şi, eventual, clienţii deserviţi de către aceştia. Pe acest fond, uneori prin forţa împrejurărilor, telesalariatul este în situaţia de a efectua muncă de noapte, aspect care atrage incidenţa dispoziţiilor imperative protective regăsite în art. 125-128 din Codul muncii.

3.6. Suplimentar, apreciem că se impune reglementarea dreptului la deconectare („R2D"), după modelul altor state membre ale UE (Franţa, Belgia, Spania, Italia)[29]. Cu privire la acesta, la nivel european există o preocupare mai

[27] Observăm că, din această perspectivă, dreptul intern impune un standard de protecţie mai ridicat decât cel reglementat de Directiva 2003/88/CE (care stabileşte că orice lucrător trebuie să beneficieze de o perioadă minimă de repaus zilnic de 11 ore consecutive în decursul unei perioade de 24 de ore (art. 3) şi, în decursul unei perioade de şapte zile, de o perioadă minimă de repaus neîntrerupt de 24 de ore, la care se adaugă cele 11 ore de repaus zilnic (art. 5)).

[28] Aspect care poate pune probleme şi în privinţa identificării *lex contractus* şi/sau *lex fori*, după caz.

[29] Pentru detalii privind R2D, a se vedea, spre exemplu, O. Vargas-Llave et al., *Right to disconnect in the 27 EU Member States*, Eurofound Working Paper, 2020, [Online] la https://www.eurofound.europa.eu/sites/default/files/ wpef20019.pdf, accesat 29.09.2021; T. Weber, *Right to disconnect: Exploring company practices*, Eurofound Research Report, 2021, [Online] la https://www.eurofound.europa.eu/sites/ default/files/ef_publication/field_ef_ document/ef21049en.pdf, accesat 29.09.2021.

veche, concretizată într-o propunere de directivă[30] care, în esenţă, vizează cerinţele minime care să le permită lucrătorilor care utilizează instrumente digitale, inclusiv TIC, în scopuri profesionale, să îşi exercite dreptul de a se deconecta şi să garanteze că angajatorii respectă acest drept.

Dreptul la deconectare ar presupune, în esenţă, dreptul de a nu se implica în activităţi sau comunicări legate de activitatea profesională prin intermediul unor instrumente digitale, direct sau indirect, în afara timpului de lucru. În sensul propunerii de directivă, statele membre vor trebui să se asigure că angajatorii instituie un sistem obiectiv, fiabil şi accesibil care să permită măsurarea duratei timpului de lucru zilnic al fiecărui lucrător, în conformitate cu dreptul lucrătorilor la viaţă privată şi la protecţia datelor lor cu caracter personal.

În privinţa măsurilor concrete de punere în aplicare a dreptului de a se deconecta statele membre ar trebui să reglementeze o serie de aspecte importante, printre care:

(a) modalităţile practice de închidere a instrumentelor digitale folosite în scopuri profesionale, inclusiv a oricărui tip de instrumente de monitorizare în scopuri profesionale;

(b) sistemul de măsurare a timpului de lucru;

(c) evaluări în materie de sănătate şi securitate, inclusiv evaluări ale riscurilor psihosociale, legate de dreptul de a se deconecta;

(d) criteriile pe baza cărora se acordă angajatorilor orice derogare de la obligaţia de a pune în aplicare dreptul lucrătorilor de a se deconecta.

În sfârşit, apreciem că reglementarea dreptului la deconectare nu exclude posibilitatea de a se efectua ore suplimentare, în condiţiile legii. Munca suplimentară poate fi programată prin acordul scris al părţilor având astfel caracter previzibil. În acest mod, propunerea angajatorului nu poate interveni intempestiv, cu risc de afectare a calităţii timpului de repaus al telesalariatului.

4. Consideraţii finale

Prin adoptarea Legii nr. 81/2018 s-a făcut un prim pas important pentru adaptarea cadrului normativ la evoluţia raporturilor de muncă în cadrul cărora sunt utilizate tehnologii moderne de comunicare la distanţă. Înainte de debutul pandemiei, riscurile păreau mai mult teoretice, iar fenomenul avea oricum o dimensiune redusă în România comparativ cu alte state europene[31].

[30] A se vedea Rezoluția Parlamentului European din 21 ianuarie 2021 conținând recomandări adresate Comisiei privind dreptul de a se deconecta (2019/2181(INL)), [Online] la https://www.europarl.europa.eu/doceo/document/TA-9-2021-0021_RO.html, accesat 29.09.2021.

[31] A se vedea, spre exemplu, Eurostat, *Working from home in the EU*, publicat la 20.06.2018, [Online] la https://ec.europa.eu/eurostat /web/products-eurostat-news/-/DDN-20180620-1, accesat 29.09.2021. Conform acestui material, în anul 2018 doar 0,4% din lucrătorii din România lucrau în mod obișnuit de la domiciliu, media la nivelul UE fiind de 5,7%. Chiar dacă pandemia COVID-19 a determinat o creștere semnificativă a acestui procent, acesta a rămas totuși foarte redus comparativ cu evoluția mediei la nivelul UE.

Se poate considera că aspectele pozitive sunt mai pregnante când acest tip de activitate este agreat de părţi fără constrângeri, în aceste situaţii salariatul având şi un capital de negociere mai consistent. Pe acest fond, prin adoptarea legii, România s-a alăturat statelor care au abordat reglementarea telemuncii având în vedere mai degrabă avantajele pe care aceasta în mod potenţial le implică, în special din perspectiva echilibrului între profesie şi viaţa privată (alături de Germania, Polonia, Portugalia, Lituania, Malta ş.a.)[32].

Prin raportare la această finalitate, trebuie subliniat că şi Directiva 2019/1158 privind echilibrul dintre viaţa profesională şi cea privată a părinţilor şi îngrijitorilor şi de abrogare a Directivei 2010/18/UE a Consiliului[33] are în vedere utilizarea unor formule de muncă la distanţă, acolo unde este posibil, ca soluţie pentru ca lucrătorii care sunt părinţi şi îngrijitorii[34] să poată să-şi adapteze programul de muncă în funcţie de necesităţile şi preferinţele personale şi, astfel, să rămână în câmpul muncii. În acest context este aşteptată completarea cadrului normativ intern, inclusiv a Legii nr. 81/2018, în procesul de transpunere atât a acestei directive, cât şi a Directivei 2019/1152 privind transparenţa şi previzibilitatea condiţiilor de muncă în Uniunea Europeană[35], de asemenea relevantă pentru raporturile de muncă la distanţă.

În prezent se poate observa că problematica atrasă de telemuncă este una mai vastă decât a prevăzut legiuitorul în anul 2018. Criza pandemică a forţat într-o anumită măsură desfăşurarea de activităţi de la distanţă ca soluţie de răspuns şi de compromis faţă de perspectiva răspândirii SARS COV2 şi faţă de riscul pierderii locurilor de muncă.

Timpul de muncă la distanţă prezintă unele valenţe diferite după cum acest tip de activitate se desfăşoară conjunctural, în context de criză, sau independent de diverşi factori constrângători.

Astfel, dacă apelul la telemuncă intervine ca soluţie temporară pentru salvarea locurilor de muncă pe fond de diminuare a activităţii angajatorilor, cu sau fără reducerea programului, părţile ar putea beneficia de flexibilitate crescută (inclusiv prin prisma programului de lucru), iar îndeplinirea sarcinilor de serviciu nu va presupune o intensitate crescută determinată de modificarea locului muncii. Dacă, dimpotrivă, ca reacţie la schimbările din mediul economic, unele domenii sunt mutate în mediul virtual, accelerându-se procesul de digitalizare (spre exemplu segmentul distribuţiei de produse, unele servicii), activitatea telesalariaţilor ar putea fi mai intensă, fie ca urmare a elementelor de noutate sau necesităţii

[32] A se vedea și European Agency for Safety and Health at Work, *Regulating telework in a post-COVID-19 Europe* (2021), [Online] la https://euagenda.eu/upload/publications/telework--20post-covid.pdf, p. 12, accesat 29.09.2021.

[33] *Termen de conformare:* 2 august 2022.

[34] Conform art. 3 alin. (1) lit. d)din directiva menționată, prin „îngrijitor" se înțelege un lucrător care oferă îngrijire sau sprijin personal unei rude sau unei persoane care locuiește în aceeași gospodărie cu lucrătorul și care are nevoie de îngrijire sau sprijin semnificativ ca urmare a unei probleme medicale grave, astfel cum este definită de fiecare stat membru.

[35] *Termen de transpunere:* 1 august 2022.

de competenţe digitale crescute cu care se confruntă, fie pentru că activitatea angajatorilor suportă modificări şi/sau are un trend ascendent.

Independent de efectele prin prisma intensităţii muncii, telemunca având caracter parţial forţat de situaţia de criză economică, mediul familial al telesalariaţilor nu mai poate fi privit în mod necesar ca un avantaj, fiind posibil ca mediul de lucru de acasă să nu fie adecvat (spaţiu insuficient sau impropriu, resimţirea unor servituţi care ţin de viaţa personală etc.). De asemenea, riscul unui conflict între viaţa profesională şi viaţa personală poate fi apreciat ca fiind mai ridicat în cazul telemuncii neplanificate, *ad hoc*.

Cu toate aceste variabile şi riscuri, telemunca a constituit şi constituie o experienţă pozitivă şi o soluţie viabilă în timpul crizei COVID pentru ambele părţi, salariaţi şi angajatori, fiind dezirabilă în multe situaţii şi în perspectivă post-pandemică[36].

Ne preocupă în mod deosebit, din perspectiva timpului de muncă, specificul telemuncii atunci când aceasta este o opţiune realizată fără constrângeri exterioare prin mijloace electronice de comunicare la distanţă.

În Rezoluţia Parlamentului European din 21 ianuarie 2021 conţinând recomandări adresate Comisiei privind dreptul de a se deconecta (2019/2181(INL)) se face referire la „apariţia unei culturi de a fi „conectat în permanenţă", „mereu online" sau „mereu de serviciu", care poate influenţa negativ drepturile fundamentale ale lucrătorilor şi condiţiile de muncă echitabile, inclusiv remunerarea echitabilă, limitarea timpului de lucru, echilibrul dintre viaţa profesională şi cea privată, sănătatea fizică şi mentală, securitatea în muncă". În mod deosebit se subliniază intensificarea muncii şi prelungirea programului de lucru, estompând astfel limitele dintre viaţa profesională şi cea privată. Din această perspectivă, sunt indicate cercetări Eurofound din care rezultă că 27% dintre respondenţii care lucrează de acasă au declarat că au lucrat în timpul liber pentru a îndeplini sarcini profesionale şi că există o probabilitate de peste două ori mai mare ca persoanele care lucrează în mod obişnuit de acasă să lucreze în plus faţă de cele 48 de ore săptămânale prevăzute şi să se odihnească mai puţin de cele 11 ore prevăzute între zilele lucrătoare.

Alte studii indică faptul că mai puţin de 60% dintre lucrătorii la distanţă, atât bărbaţi, cât şi femei, lucrează la „orele obişnuite", faţă de aproximativ 80% dintre lucrătorii comparabili care desfăşoară activităţi la locurile de muncă organizate de către angajatori[37].

Pe de altă parte, s-a apreciat că deşi, în general, telesalariaţii par să lucreze „ore mai lungi" şi mai mult suplimentar faţă de cei care desfăşoară activităţi la locul de muncă organizat de angajator, totuşi, această concluzie nu se verifică în cazul în

[36] Pentru statistici în acest sens, a se vedea D. Ahrendt et. al., *Living, working and COVID-19*, Eurofound Research Report, 2020, [Online] la https://www.eurofound. europa.eu/ sites/default/files/ef_publication/field_ef_document/ ef20059en.pdf, accesat 29.09.2021.

[37] J.I. Giménez-Nadal, J.A. Molina, J. Velilla, *Telework, the Timing of Work, and Instantaneous Well-Being: Evidence from Time Use Data*, publicat în ianuarie 2018, [Online] la https://ftp.iza.org/dp11271.pdf, accesat 29.09.2021.

care sunt comparaţi cu acei salariaţi care nu lucrează de la distanţă, dar li s-a oferit această alternativă şi au refuzat-o. Drept urmare, s-a sugerat că nu telemunca în sine este „responsabilă" pentru durata sau intensitatea muncii, ci mai curând natura postului şi/sau condiţiile impuse de angajator pentru activitatea care poate fi prestată şi de la distanţă (în special sistemul de remunerare axat mai puţin pe recompensarea timpului suplimentar şi mai mult pe acordarea de bonusuri pentru atingerea unor obiective de performanţă). S-a mai apreciat, pe cale de consecinţă, că nu există motive pentru a se presupune că munca la domiciliu va duce automat la intensificarea muncii şi la mai multe ore suplimentare[38].

După cum se poate observa, analiza timpului de muncă la distanţă poate urma parametri diverşi: natura postului şi a activităţii, predispoziţia sau nevoia de a lucra suplimentar, percepţia asupra timpului, lucrul în cadrul programului obişnuit sau în afara acestuia, timpul de desfăşurare a unei activităţi în mod efectiv sau timp la dispoziţia angajatorului ş.a.

Se poate afirma cu grad ridicat de certitudine că telemunca este potenţată de dezvoltările tehnologice şi potenţează forme contractuale de tip *on call* sau *platform work*. S-a arătat şi că munca la domiciliu produce efecte asupra organizării muncii, asupra duratei şi predictibilităţii programului de lucru, conducând la estomparea graniţelor dintre timpul de muncă şi cel de repaus[39].

Lucrul de la distanţă mai poate determina o tendinţă de depersonalizare a relaţiei telesalariat - angajator, lipsa percepţiei acurate a eforturilor salariatului din timpul programului de lucru, cu potenţiale efecte în sensul supranormării sau a concentrării pe rezultatul activităţii, uneori cu ignorarea perioadelor în care salariatul este la dispoziţia angajatorului/clienţilor acestuia.

Într-un alt plan, acest tip de activitate poate fie să crească nivelul de armonie dintre viaţa profesională şi cea privată, fie, dimpotrivă, să conducă la instabilitate sau la accentuarea unor dezechilibre latente sau minore. Conştientizarea potenţialelor avantaje şi riscuri, respectarea timpului de muncă şi de odihnă, trebuie să constituie în egală măsură preocupări ale telesalariaţilor.

Pe acest fond, în mod special, aspectele privind programul de lucru, evidenţa, monitorizarea timpului de lucru şi dreptul la deconectare trebuie să fie avute în vedere prin reglementări protective care să nu se limiteze la a lăsa aceste aspecte la dispoziţia părţilor (mai ales în condiţiile în care, în perioade de criză, vulnerabilitatea salariaţilor este mai ridicată şi, pe cale de consecinţă, consimţământul acestora mai uşor de obţinut).

În mod special mijloacele de evidenţă a muncii trebuie să exprime nivelul de tehnologizare a muncii, iar sancţiunile aplicabile în caz de nerespectare a standardelor minimale privind timpul de muncă trebuie să fie eficiente, disuasive.

[38] P. Peters, C. Wetzels, K. Tijdens, *Telework: Timesaving or Time-Consuming? An Investigation onto Actual Working Hours*, The Journal of Interdisciplinary Economics, 2008, Vol. 19, pp. 421–442.

[39] În acest sens şi Raportul OIM, *Ensuring decent working time for the future*, *cit. supra.*

Referinţe

Ahrendt D.et. al., *Living, working and COVID-19*, Eurofound Research Report, 2020

Ciobiriciu Ştefănescu A., *Telemunca*, în Revista Română de Dreptul Muncii, nr. 1/2009

Dima L., *Aspecte de noutate privind mijloacele materiale de probă în contextul noilor tehnologii*, în *Conferinţa Internaţională de Dreptul Muncii - Noile tehnologii, consecinţe asupra raportului de muncă*, Sibiu, 11-12 octombrie 2019, Editura Universul Juridic, Bucureşti, 2020

Eurostat, *Working from home in the EU*, publicat la 20.06.2018

European Agency for Safety and Health at Work, *Regulating telework in a post-COVID-19 Europe* (2021)

Gheorghe M., *Munca prestată prin utilizarea platformelor digitale. Consecinţe asupra principiului egalităţii de tratament*, în *Conferinţa Internaţională de Dreptul Muncii - Noile tehnologii consecinţe asupra raportului de muncă*, Sibiu, 11-12 octombrie 2019, Editura Universul Juridic, Bucureşti, 2020

Giménez-Nadal J.I., Molina J.A., Velilla J., *Telework, the Timing of Work, and Instantaneous Well-Being: Evidence from Time Use Data*, publicat în ianuarie 2018, http://dx.doi.org/10.2139/ssrn.3111144

Marica M.E., *Contracte de muncă atipice*, Editura Universul Juridic, Bucureşti, 2019

Moarcăş C.A., *Efectele globalizării, transformarea relaţiei de muncă şi regândirea dialogului social*, în Revista Română de Drept Privat, nr. 4/2019

Nenu C.C., *Evoluţia conceptului de securitate şi sănătate în muncă în contextul noilor tehnologii*, în *Conferinţa Internaţională de Dreptul Muncii Noile tehnologii consecinţe asupra raportului de muncă*, Sibiu, 11-12 octombrie 2019, Editura Universul Juridic, Bucureşti, 2020

Panainte S., *Consideraţii privind alienarea salariatului în industria 4.0.*, în *Conferinţa Internaţională de Dreptul Muncii - Noile tehnologii consecinţe asupra raportului de muncă*, Sibiu, 11-12 octombrie 2019, Editura Universul Juridic, Bucureşti, 2020

Peters P., Wetzels C., Tijdens K., *Telework: Timesaving or Time-Consuming? An Investigation onto Actual Working Hours*, The Journal of Interdisciplinary Economics, 2008, Vol. 19, https://doi.org/10.1177%2F02601079X08001900407

Raportul Eurofound, *Telework in the European Union*, publicat la 10.01.2010

Raportul OIM, *Ensuring decent working time for the future*, International Labour Conference, 107th Session, 2018, *General Survey concerning working-time instruments*, Geneva, 2018, Report of the Committee of Experts on the Application of Conventions and Recommendations (articles 19, 22 and 35 of the Constitution), Report III (Part B)

Rezoluţia Parlamentului European din 21 ianuarie 2021 conţinând recomandări adresate Comisiei privind dreptul de a se deconecta (2019/2181(INL))

Samek Lodovici M. *et al., The impact of teleworking and digital work on workers and society. Special focus on surveillance and monitoring, as well as on mental health of workers*, 2021, publication for the Committee on Employment and Social Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament

Servais J.M., *Economia colaborativă a platformelor electronice: noi provocări, noi protecţii*, în *Conferinţa Internaţională de Dreptul Muncii - Noile tehnologii consecinţe asupra raportului de muncă*, Sibiu, 11-12 octombrie 2019, Editura Universul Juridic, Bucureşti, 2020

Ştefănescu A., *Munca la domiciliu şi telemunca. Drept intern şi comparat*, Editura Universul Juridic, Bucureşti, 2011

Ţichindelean M., *Consideraţii privind protecţia datelor cu caracter personal în raporturile de muncă prin utilizarea mijloacelor de supraveghere video*, în *Conferinţa Internaţională de Dreptul Muncii - Noile tehnologii consecinţe asupra raportului de muncă*, Sibiu, 11-12 octombrie 2019, Editura Universul Juridic, Bucureşti, 2020

Vargas-Llave O. et al., *Right to disconnect in the 27 EU Member States*, Eurofound Working Paper, 2020

Weber T., *Right to disconnect: Exploring company practices*, Eurofound Research Report, 2021

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-4

Portabilitatea datelor cu caracter personal, prin prisma dispoziţiilor RGDP şi ale Directivei 2019/770: este gambitul reginei mutarea de deschidere adecvată?

Portability of Personal Data, From the Perspective of the GDPR and Directive 2019/770 Provisions: Is the Queen's Gambit the Right Opening?

Juanita Goicovici[1]

Rezumat: Studiul abordează problematica portabilităţii datelor cu caracter personal, în perimetrul exercitării dreptului persoanei vizate de acces la datele cu caracter personal colectate şi prelucrate de către operatorii de date cu caracter personal, astfel cum este conturat în textul art. 15 din Regulamentul General nr. 679 din 27 aprilie 2016 privind protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. Exercitarea dreptului la portabilitatea datelor cu caracter personal nu implică doar efecte insulare, ci antamează efecte de tip arhipelag, prin prisma faptului că se poziţionează în prima linie a exercitării efective a altor drepturi esenţiale ale persoanei vizate, în optica dispoziţiilor GDPR şi ale Directivei 2019/770, condiţionând implicit, într-o măsură considerabilă, exercitarea dreptului de acces la datele cu caracter personal, dreptul la rectificare a datelor cu caracter personal şi dreptul de a se opune prelucrării datelor cu caracter personal. Controlul exercitat de persoana vizată asupra prelucrării datelor cu caracter personal şi participarea activă a persoanei vizate la actualizarea preferinţelor sale în ceea ce priveşte consimţământul la prelucrarea datelor cu caracter personal, inclusiv decizia de a transfera datele cu caracter personal către un alt operator îşi găsesc expresia normativă în binomul reprezentat de dreptul de acces al persoanei vizate şi dreptul la portabilitatea datelor. Portabilitatea datelor necesită punerea în aplicare a standardelor tehnice pertinente, în ceea ce priveşte adecvarea mecanismului care vizează facilitarea transferului de date între operatori, inclusiv prin prisma capacităţii de a exporta datele utilizatorului într-un fişier digital accesibil utilizatorului, promovând astfel interoperabilitatea, precum şi facilitarea identificării datelor şi controlul efectiv al persoanei vizate asupra procesării datelor cu caracter personal.

Cuvinte-cheie: portabilitate; date personale; drept de acces; drept de restricţionare; drept de opoziţie

[1] Lector univ. dr., Facultatea de Drept, Universitatea „Babeş-Bolyai” din Cluj-Napoca, e-mail: juanita.goicovici@law.ubbcluj.ro. Textul studiului preia argumentele susținute în cadrul Conferinței internaționale „Perspective juridice asupra Internetului. Spațiul virtual, ultima frontieră? Încheierea și executarea contractelor”, ediția a 5-a, Iași, 30-31 oct. 2021.

Abstract: The study addresses the issue of the personal data portability, in the perimeter of the exercising of the data subject's right of access to personal data collected and processing by personal data controllers, as outlined in the text of art. 15 of Regulation no. 679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The exercise of the right of personal data portability does not imply merely insular effects, since it consequentially engages archipelago effects, as it is at the forefront of the effective exercise of other essential rights of the data subject, in the light of the GDPR and Directive 2019/770 provisions, implicitly conditioning, to a considerable extent, the exercise of the right of access to personal data, the right to rectification of personal data and the right to oppose the processing of personal data. The subject's control exercised over the personal data processing concerning the active participation of the data subject in updating his / her preferences in terms of consenting to personal data processing, including the decision to port the personal data to another controller, find their normative expression in the binomen represented by the data subject's right of access and the right of data portability. Data portability requires the implementing of pertinent technical standards, in terms of adequacy and appropriateness of mechanism aimed at the facilitating of the transfer from one data controller to another, such as the ability to export user data into a user-accessible local file, thus promoting interoperability, as well as facilitating searchability and data subject's effective control over data processing.

Keywords: portability; personal data; right of access; right of restriction; right of opposition

1. Remarci introductive

Ipostaziindu-se ca expresie a dreptului persoanei vizate de a-şi retrage oricând, în orice moment, consimţământul furnizat voluntar cu privire la colectarea şi prelucrarea datelor cu caracter personal care o privesc, calibrată ca mecanism de control[2] al persoanei vizate asupra propriilor date personale, portabilitatea datelor

[2] A se consulta, pentru detalii, P. de Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez, *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, Computer Law & Security Review, 2018, pp. 193–203, [Online] la https://ssrn.com/abstract=3447060, accesat 08.11.2021; A. de Streel, J. Kraemer, P. Senellart, *Making Data Portability More Effective for the Digital Economy* (June 14, 2021), [Online] la https://ssrn.com/abstract=3866495, accesat 08.11.2021; D. Gill, W. Kerber, *Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data* (October 11, 2020), [Online] la https://ssrn.com/ abstract=3715357, accesat 08.11.2021; I. Graef, *The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation*, Competition Policy International, Antitrust Chronicle November 2020 (II), [Online] la https://ssrn.com/abstract=3740185, accesat 08.11.2021; P. Aertgeerts, *Shaping Fundamental Rights: The Right to Data Portability, the EU Legislator and the Normative Foundations of the Fundamental Right to Data Protection* (November 6, 2019), [Online] la https://ssrn.com/abstract=3497791, accesat 08.11.2021; A. Alberini, Y. Benhamou, *Data Portability and Interoperability: An Issue that Needs to Be Anticipated in Today's It-Driven World* (August 1, 2017), [Online] la https://ssrn.com/abstract=3038877, accesat 08.11.2021; G. Araújo Souto, *Data Portability: a Necessary Right for Users and Competitors of Digital Platforms* (October 12, 2018), [Online] la https://ssrn.com/abstract=3293056, accesat 08.11.2021.

personale descrie mutabilitatea acestor date, posibilitatea de a fi transferate către un alt operator la solicitarea persoanei vizate, cu corolarul posibilităţii de a reutiliza datele personale într-un alt context digital[3].

Parcimonios în abordare, textul art. 20 din RGDP descrie aceste prerogative ca referindu-se la faptul că „Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc şi pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal", în cazurile expres prevăzute de art. 20, alin. (1), lit. a).-b). din Regulamentul General.

Descompus în prerogativele supraetajate conferite persoanei vizate, dreptul la portabilitatea datelor personale implică: (i) dreptul titularului de a primi datele personale într-un format structurat (sau aşa-numita prerogativă a persoanei vizate de prelucrare, de a recupera informaţiile cu caracter personal pe care le-a furnizat unui operator, într-o formă structurată, utilizată curent, lizibilă automat), persoană care poate păstra informaţiile pentru uz personal ori le poate transmite unui alt operator; (ii) dreptul de a transmite datele unui alt responsabil / operator, care se exercită fără ca operatorul de date precedent să poată formula o opoziţie, în acest mod, persoana vizată păstrând controlul asupra propriilor date; astfel, dreptul la portabilitate încurajează persoanele vizate să îşi recupereze datele cu caracter personal şi să le reutilizeze; (iii) dreptul la portabilitatea datelor se ipostaziază, simultan, ca expresie a dreptului persoanei vizate de retractare a consimţământului la prelucrarea datelor sale cu caracter personal[4], furnizate în primă fază operatorului de date în vederea prelucrării, în baza unui consimţământ de tip *opting-in,* componenta consimţământului *opting-out* fiind esenţială în economia prelucrării datelor conform dispoziţiilor RGDP, fondată pe consimţământul persoanei vizate. Precaritatea obţinerii acordului persoanei vizate cu privire la prelucrarea datelor

[3] C. Jugastru, *Dreptul la portabilitatea datelor*, Revista Universul Juridic, [Online] la http://revista.universuljuridic.ro/dreptul-la-portabilitatea-datelor/, accesat 08.11.2021.

[4] Pentru dezvoltări, a se consulta C. Banda, *Enforcing Data Portability in the Context of EU Competition Law and the GDPR*, MIPLC Master Thesis Series 2017, [Online] la https://ssrn.com/abstract=3203289, accesat 08.11.2021; I. Graef, D. Clifford, P. Valcke, *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law,* International Data Privacy Law, vol. 8, nr. 3/2018, pp. 200-223, [Online] la https://ssrn.com/abstract=3216198, accesat 08.11.2021; J. Belo, P. Macedo Alves, *The Right to Data Portability: An In-Depth Look,* Journal of Data Protection and Privacy, Vol. 2, nr. 1/2018, pp. 53-61, [Online] la https://ssrn.com/abstract=3541656, accesat 08.11.2021; M. Borghi, *Data Portability and Regulation of Digital Markets,* CIPPM / Jean Monnet Working Papers, Bournemouth University, 2019, [Online] la https://ssrn.com/abstract=3617792, accesat 08.11.2021; E. Bozdag, *Data Portability Under GDPR: Technical Challenges* (January 28, 2018), [Online] la https://ssrn.com/ abstract=3111866, accesat 08.11.2021; I. Graef, M. Husovec, J. van den Boom, *Spill-Overs in Data Governance: The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes*, TILEC Discussion Paper No. DP 2019-005, 2019, [Online] la https://ssrn.com/abstract=3369509, accesat 08.11.2021.

personale care o privesc, ca şi caracterul eminamente provizoriu al acestui acord asupra colectării şi prelucrării, implică, pentru operatorii de date, obligaţia de a informa utilizatorii cu privire la existenţa dreptului la portabilitate, dublată de obligaţia de a onora cererea de portabilitate a utilizatorului în cel mai scurt timp posibil, însă fără să depăşească o lună de la data solicitării, sau, în cazurile complexe, fără să poată depăşi un interval de trei luni de la data primirii cererii de portare, cu condiţia ca operatorul să informeze utilizatorul despre motivele care duc la întârzierea onorării cererii, în termen de o lună, respectiv obligaţia operatorului de a răspunde cererii utilizatorului de portare a datelor / de accesare a acestora într-un format structurat, chiar dacă acest răspuns este unul negativ (de refuz), în ipotezele (limitate) în care refuzul ar fi unul legitim.

Ne propunem, în paragrafele care urmează, să abordăm, mai întâi, prerechizitele exercitării dreptului la portabilitatea datelor, prin prisma controlului exercitat de persoana vizată asupra prelucrării datelor cu caracter personal, precum şi din unghiul elementelor care caracterizează participarea activă, asertivă a persoanei vizate la actualizarea preferinţelor sale în ceea ce priveşte consimţământul la prelucrarea datelor cu caracter personal, inclusiv în ceea ce priveşte decizia de a transfera datele cu caracter personal către un alt operator (i), urmând ca, într-o secţiune distinctă, să ne oprim asupra problematicii suprapunerii parţiale şi a imbricaţiilor semnalate între dispoziţiile art. 20 RGDP şi prevederile Directivei 2019/770 în materia conformităţii conţinutului digital (ii).

1.1. Portabilitatea datelor cu caracter personal: efecte de tip insular vs. efecte de tip arhipelag

Calibrată ca prerogativă de control al titularului asupra prelucrării datelor sale personale, portabilitatea datelor se bifurcă în dreptul unei persoane fizice „de a primi datele cu caracter personal care o privesc şi pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent şi care poate fi citit automat" (i) şi, pe celălalt versant, în dreptul de a transmite aceste date altui operator, fără obstacole nejustificate din partea operatorului căruia i-au fost furnizate datele cu caracter personal (ii), fiind, din start, excluse din sfera materială de incidenţă a acestui drept datele anonimizate sau datele care nu privesc utilizatorul care solicită accesul[5]; datele pseudonimizate (care, prin definiţie, pot fi

[5] Noțiunea de „date furnizate de către utilizator" trebuie interpretată și înțeleasă în mod extensiv, după cum s-a evidențiat în literatura de specialitate, astfel încât s-a admis că aceasta cuprinde toate datele deținute de către operator cu privire la persoana utilizatorului, cu excepția datelor inferate sau derivate. În acest sens, sunt incluse, pe de o parte, datele personale furnizate în mod activ de către utilizator prin mijloacele tehnice puse la dispoziție de către operator, ca, de exemplu, datele privitoare la adresa de e-mail, vârstă, locație, număr de telefon, adresă poștală, nume utilizator, cod numeric personal etc. (a), precum și datele rezultate din activitatea utilizatorului, cum ar fi: datele privind locația, pulsul acestuia și valorile tensiunii arteriale, istoricul de căutări pe o pagină web, paginile web accesate etc. După cum s-a subliniat, însă, cu privire la datele inferate sau derivate din datele oferite operatorului de către utilizator, acesta din urmă nu beneficiază de dreptul la

folosite pentru a identifica utilizatorul, chiar dacă identificarea se face cu ajutorul unor chei de decriptare) fac obiectul dreptului la portarea datelor, pseudonimizarea nereprezentând *per se* un obstacol în calea exercitării acestor prerogative. Obligaţiile operatorului de date, aflate în corelaţie cu exerciţiul dreptului la portabilitate, se defalcă în obligaţia de a informa utilizatorii cu privire la existenţa dreptului la portabilitate (a), obligaţia de a pune la dispoziţia utilizatorului, la cererea acestuia, o versiune a datelor furnizate de către acesta într-un format accesibil şi reutilizabil (b), operatorul fiind, de asemenea, obligat să onoreze cererea utilizatorului în cel mai scurt timp posibil, însă fără să depăşească o lună de la data solicitării, sau, în cazurile complexe, nu mai mult trei luni de la momentul amintit, cu condiţia ca operatorul să informeze utilizatorul despre motivele care conduc la întârzierea onorării cererii în termenul de o lună (c); operatorului de date îi incumbă, totodată, obligaţia să răspundă cererii utilizatorului, chiar dacă acest răspuns este unul negativ, de refuz al accesului la date într-un format portabil[6] (d); se cuvine reamintit că operatorul poate refuza onorarea unei astfel de cereri a utilizatorului dacă aceasta este nefondata sau dacă are un caracter repetitiv la intervale nerezonabile de timp (ori le poate onora contra unui cost rezonabil); este util de menţionat, de asemenea, că aceste cereri nu pot fi considerate ca fiind excesive dacă, prin natura activităţii sale, operatorul oferă servicii de informare sau procesare automată a datelor personale. Cu titlu de principiu, operatorul de date trebuie să onoreze cererile de acces la date şi de portare în mod gratuit[7] (cu excepţia

portabilitate. Pentru detalii, a se consulta I. Graef, M. Husovec, N. Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, German Law Journal, vol. 19, nr. 6/2018, pp. 1359-1398, Tilburg Law School Research Paper No. 2017/22, [Online] la https://ssrn.com/abstract=3071875, accesat 08.11.2021; J. Hurwitz, *Digital Duty to Deal, Data Portability, and Interoperability*, The Global Antitrust Institute Report on the Digital Economy 28, 2020, [Online] la https://ssrn.com/abstract=3733744, accesat 08.11.2021; T. Ke, K. Sudhir, *Privacy Rights and Data Security: GDPR and Personal Data Driven Markets* (July 5, 2020), [Online] la https://ssrn.com/abstract=3643979, accesat 08.11.2021; J. Kraemer, *Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations*, Journal of Competition Law & Economics, 2020, [Online] la https://ssrn.com/abstract=3742771, accesat 08.11.2021.

[6] A se vedea M. Leistner, *The Existing European IP Rights System and the Data Economy – An Overview With Particular Focus on Data Access and Portability*, în J. Drexl (ed.), „Data access, Consumer Protection and Public Welfare", Nomos, 2020, [Online] la https://ssrn.com/abstract=3625712, accesat 08.11.2021; P. Leonard, *Regulatory Trends and Emerging Practices in Access to Customer Data, Portability and Data Sharing in the Financial Services Sector* (December 3, 2017), [Online] la https://ssrn.com/ abstract=3154275, accesat 08.11.2021;

[7] A. Lisievici, *Dreptul la portabilitatea datelor potrivit Regulamentului General privind Protecția Datelor*, în I. Alexe, D.-N. Ploeșteanu, D.-M. Șandru, „Protecția datelor cu caracter personal. Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experienţelor româneşti şi noile provocări ale Regulamentului (UE) 2016/679", Editura Universitară, București, 2017, p. 149-153, [Online] la https://ssrn.com/abstract=3039537, accesat 09.11.2021.

cazurilor de adresare a unor cereri repetitive, pentru care poate percepe o contraprestaţie echitabilă), operatorul trebuind să ia toate măsurile de siguranţă, astfel încât datele transmise să ajungă în mod sigur (de exemplu prin utilizarea unor *encrypt keys*) la utilizatorul corect selectat, cu evitarea unor *data leaks* către persoane care nu sunt titulari ai dreptului de acces, fără ca aceste măsuri de filtrare a accesului ilegal ori de siguranţă să împiedice utilizatorii să îşi exercite drepturile privitoare la portarea datelor cu caracter personal. În ceea ce priveşte selectarea formatului adecvat, Regulamentul General recunoaşte ca format adecvat[8] orice format electronic, structurat şi codificat într-o manieră care nu limitează procesarea automată sau reutilizarea datelor şi care poate fi recunoscut uşor de către aplicaţiile *software*, costul impus de onorarea unei astfel de cereri neputând reprezenta un motiv legitim de refuz al accesului la datele cu caracter personal într-un format portabil.

1.2. Contra-gambitul: portabilitatea datelor în temeiul dispoziţiilor Directivei 2019/770 privind contractele de furnizare de conţinut digital şi de servicii digitale

După cum rezultă din Considerentul (24) al Directivei 2019/770, datele cu caracter personal pot constitui o contraprestaţie conjuncturală a furnizării conţinutului digital, în legătură cu acest aspect reţinându-se, în cuprinsul considerentului menţionat, că, în esenţă, „conţinutul digital şi serviciile digitale sunt adesea furnizate şi în cazul în care consumatorul nu plăteşte un preţ, ci îi furnizează comerciantului date cu caracter personal". Caracterul de *drept fundamental* al dreptului la protecţia datelor personale este amintit *expressis verbis* în textul Considerentului (24) al Directivei 2019/770, cu indicarea explicită a faptului că datelor personale, dacă le poate fi imprimat regimul de bunuri aflate în circuitul civil / comercial[9], acest regim nu exclude (şi nici nu restrânge) protecţia juridică specială de care se bucură în opoziţie cu statutul altor bunuri incorporale[10].

[8] A. G. Monteleone, *Il Diritto Alla Portabilità Dei Dati. Tra Diritti Della Persona e Diritti Del Mercato*, LUISS Law Review, 2/2017, [Online] la https://ssrn.com/abstract=3088984, accesat 08.11.2021; G. Nicholas, *Taking It With You: Platform Barriers to Entry and the Limits of Data Portability*, Michigan Telecommunications and Technology Law Review, 2020, [Online] la https://ssrn.com/abstract=3550870, accesat 08.11.2021; P. Swire, *The Portability and Other Required Transfers Impact Assessment: Assessing Competition, Privacy, Cybersecurity, and Other Considerations,* Georgia Tech Scheller College of Business Research Paper No. 3689171, 2020, [Online] la https://ssrn.com/abstract=3689171, accesat 08.11.2021.

[9] A. Metzger, *A Market Model for Personal Data: State of Play Under the New Directive on Digital Content and Digital Services* (August 4, 2020). în S. Lohsse, R. Schulze, D. Staudenmayer (eds.), „Data as Counter-Performance – Contract Law 2.0?" Münster Colloquia on EU Law and the Digital Economy V, 2020, [Online] la https://ssrn.com/abstract=3666805, accesat 29.11.2021.

[10] În Considerentul (24) al Directivei 2019/770 se reține că: „Deși recunoaște pe deplin că protecția datelor cu caracter personal este un drept fundamental și, așadar, datele cu caracter personal nu pot fi considerate o marfă, prezenta directivă ar trebui să asigure faptul

Încorsetată între limitele descrise în Considerentul (24), situaţia în care datele cu caracter personal sunt furnizate comerciantului / vânzătorului de conţinut digital fie în momentul încheierii contractului (i), fie ulterior, de exemplu, atunci când consumatorul îşi dă consimţământul ca vânzătorul să utilizeze datele cu caracter personal pe care consumatorul le-ar putea încărca sau le-ar putea crea cu ajutorul conţinutului digital sau al serviciului digital (ii) implică numeroase interogaţii practice, în legătură cu eventuala suprapunere ori prioritizare a invocării dreptului de acces[11] la datele încărcate, într-un format portabil fie în temeiul prevederilor art. 20 RGDP, fie, dimpotrivă, în temeiul dispoziţiilor specifice incluse în Directiva 2019/770 privind contractele de furnizare a conţinutului digital.

„Gambitul" veritabil la care poate recurge utilizatorul, în aceste cazuri, va presupune invocarea prevederilor art. 20 RGDP dacă doreşte să obţină transmutarea datelor cu caracter personal într-un format portabil până la momentul rezilierii contractului de furnizare a conţinutului digital / serviciilor digitale, moment de la care s-ar putea prevala de dispoziţiile Directivei 2019/770 pentru a obţine portarea datelor / fişierelor încărcate ori create cu ajutorul conţinutului digital contractat, incluzând eventualele date cu caracter personal astfel utilizate.

că, în contextul acestor modele de afaceri, consumatorii au dreptul la măsuri corective contractuale. Prin urmare, prezenta directivă ar trebui să se aplice contractelor în care comerciantul furnizează sau se angajează să furnizeze conţinut digital sau un serviciu digital consumatorului, iar consumatorul furnizează sau se angajează să furnizeze date cu caracter personal. Datele cu caracter personal ar putea fi furnizate comerciantului fie în momentul încheierii contractului, fie ulterior, de exemplu, atunci când consumatorul își dă consimțământul ca respectivul comerciant să utilizeze datele cu caracter personal pe care consumatorul le-ar putea încărca sau le-ar putea crea cu ajutorul conținutului digital sau al serviciului digital. Dreptul Uniunii privind protecția datelor cu caracter personal prevede o listă cuprinzătoare de temeiuri juridice pentru prelucrarea legală a datelor cu caracter personal. Prezenta directivă ar trebui să se aplice oricărui contract în care consumatorul furnizează sau se angajează să furnizeze comerciantului date cu caracter personal. De exemplu, prezenta directivă ar trebui să se aplice în cazul în care consumatorul deschide un cont pe o platformă de comunicare socială și pune la dispoziția comerciantului numele și adresa de e-mail, care sunt folosite și pentru alte scopuri decât simpla furnizare a conținutului digital sau a serviciului digital sau respectarea cerințelor legale. Prezenta directivă ar trebui să se aplice, de asemenea, și în cazul în care consumatorul își dă consimțământul ca orice material care constituie date cu caracter personal, cum ar fi fotografiile sau postările pe care le încărcă, să fie prelucrate de comerciant în scopuri de marketing. Totuși, statele membre ar trebui să dispună de libertatea de a decide dacă sunt respectate dispozițiile de drept intern privind încheierea, existența și valabilitatea contractelor."

[11] H. Vrabec, *The Failure of Control Rights in the Big Data Era – Does a Holistic Approach Offer a Solution?*, in M. Bakhoum, B. Gallego Conde, M.-O. Mackenordt, G. Surblyte (eds.) „Personal Data in Competition, Consumer Protection and IP Law – Towards a Holistic Approach?", Berlin Heidelberg: Springer, 2017, [Online] la https://ssrn.com/abstract=3134745, accesat 08.11.2021;

1.3. *In unum locum colliguntur:* situaţii incluse şi situaţii exceptate din sfera dreptului de a obţine portarea datelor personale

Controlul exercitat de persoana vizată asupra prelucrării datelor cu caracter personal, ca şi participarea activă, asertivă a persoanei vizate la actualizarea preferinţelor sale în ceea ce priveşte consimţământul la prelucrarea datelor cu caracter personal, inclusiv decizia de a transfera datele cu caracter personal către un alt operator, îşi găsesc expresia normativă în binomul reprezentat de dreptul de acces al persoanei vizate şi dreptul la portabilitatea datelor. Portabilitatea datelor personale este condiţionată, frecvent, de prerechizitele tehnice privind punerea în aplicare a standardelor tehnice pertinente, în ceea ce priveşte adecvarea mecanismului care vizează facilitarea transferului de date între operatori, inclusiv prin prisma capacităţii de a exporta datele utilizatorului într-un fişier digital accesibil utilizatorului, promovând astfel interoperabilitatea, precum şi facilitarea identificării datelor şi controlul efectiv al persoanei vizate asupra procesării datelor cu caracter personal.

Dispoziţiile art. 20 din Regulamentul General indică un triptic de situaţii exceptate din sfera exerciţiului dreptului de a obţine portarea datelor personale. Pe un prim palier, este de semnalat că dreptul la portabilitate se aplică numai datelor aflate în posesia operatorului la momentul procesării cererii de acces / de portare, astfel încât devine un truism aserţiunea conform căreia, dacă persoana vizată şi-a exercitat anterior dreptul la uitare (dreptul la ştergerea datelor) în temeiul art. 17 RGDP, titularul nu poate adresa simultan / ulterior o solicitare de portare a datelor. Acelaşi efect poate fi semnalat şi pentru datele care au fost anonimizate şi nu mai aparţin unei persoane identificabile, la momentul înregistrării cererii de acces la date într-un format portabil. Observaţia enunţată în literatura de specialitate[12] este pertinentă şi merită accentuată: operatorului de date nu îi incumbă, însă, automat obligaţia ştergerii datelor cu caracter personal, ca urmare a primirii solicitării de portare, în măsura în care şi atât timp cât datele respective sunt necesare pentru executarea în continuare a contractului, după cum nu îi revine operatorului nici obligaţia de a menţine[13] datele cu caracter personal peste durata stabilită iniţial,

[12] A se vedea S. Turner, J. Galindo Quintero, J. Lis, L. Tanczer, *The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment* (September 26, 2021), [Online] la SSRN: https://ssrn.com/abstract=3931040, accesat 08.11.2021; S. Vezzoso, *Competition Policy in Transition: Exploring Data Portability's Roles*, 15th ASCOLA Conference, 25-27 June 2020, [Online] la https://ssrn.com/abstract=3634736, accesat 08.11.2021.

[13] În literatura de specialitate, s-a subliniat că: *"A final remark should be dedicated to the balancing provisions of Article 20(3). It may happen that data controllers, in order to comply with users' requests of data portability, could adopt specific technologies (data trackers, personal data identifiers, etc.) in processing operations that could appear as unfeasible for a full erasure of personal data. Another risk might be that, in order to guarantee a full exercise of the right to data portability to all users, data subjects whose data are inseparable from other subjects' data could be prevented from having their data erased. In all these cases, Article 20(3)*

corelată cu scopurile prelucrării (în aşteptarea unor potenţiale solicitări de portare); de asemenea, este deja un truism faptul că operatorului de date nu îi revine obligaţia de a utiliza formate digitale compatibile cu ale altor operatori. Pe celălalt versant al discuţiei, dreptul la portabilitate nu poate interfera cu o sarcină a prelucrării datelor îndeplinită de operator în interes public. În cel de-al treilea rând, portabilitatea nu va afecta negativ drepturile şi libertăţile altora, ca limită enunţată expres în cuprinsul art. 20 RGDP.

Recognoscibilă în special prin faptul că datele cu caracter personal a căror portare este solicitată sunt plasate, la acel moment, în interconectivitate cu datele personale ale altor persoane vizate[14] (începând cu exemplul clasic al unei imagini în care figurează mai multe persoane ori exemplul unui raport de activitate procesat de angajator în care au fost evaluate performanţele mai multor salariaţi etc.[15]), cea de a treia excepţie de la regula portabilităţii datelor cu caracter personal intervine în ipoteza în care persoana vizată, care a solicitat portarea datelor, a furnizat aceste date operatorului iniţial[16], iar un posibil răspuns afirmativ ar putea implica lezarea drepturilor altor persoane ori, cel puţin, bruscarea într-o manieră nerezonabilă ori inadecvată a aşteptărilor rezonabile ale celorlalte persoane vizate implicate. În acest din urmă caz, exercitarea dreptului la portabilitatea datelor personale nu poate fi acomodată cu prerogativele de control aparţinând altor persoane implicate, ceea ce impune, pe cale de consecinţă, refuzul legitim al operatorului de a da curs cererii de acces ori de portare a datelor[17].

Dreptul la portabilitatea datelor este uzual descris ca reprezentând prerogativa persoanei vizate, de a recupera informaţiile cu caracter personal (pe care le-a furnizat unui operator), într-o formă structurată, utilizată curent, lizibilă automat în format digital, cu posibilitatea ca datele respective să fie transferate altui operator, operatorul căruia i-au fost furnizate iniţial datele fiind ţinut să nu obstaculeze prin blocaje inutile deplasarea, copierea sau, după caz, transmiterea

states a prevalence of right to erasure on the right to data portability"; fragmentul este preluat din lucrarea P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez, *op. cit.*, p. 198.

[14] *Ibidem;* autorii citaţi consideră, pornind de la sintagma *"adversly exercised"* prezentă în textul art. 20 RGDP, că: *"It is irrelevant whether data portability affects other rights or freedoms; what is essential in this case is that this effect is not "adverse", e.g., it shall not create an unjustified damage or an illegitimate limitation to other rights or freedoms. In practice this means that judges will need to determine – on a case-by-case approach – when the right to data portability will adversely affect rights and freedom of others in a specific circumstance*".

[15] S. Vezzoso, *Data Portability: Initial Reflections on an Ex Ante Approach* (March 26, 2020), [Online] la https://ssrn.com/abstract=3561413, accesat 08.11.2021.

[16] *Ibidem.*

[17] Pentru detalii pe marginea acestui subiect, a se consulta H. Vrabec, *Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control,* SCRIPT-ed, 2018, [Online] la https://ssrn.com/abstract=3176820, accesat 08.11.2021; R. Walters, *The Current Status of Data Portability in Personal Data and Competition Law,* European Competition Law Review, 2020, [Online] la https://ssrn.com/abstract=3699807, accesat 08.11.2021.

datelor cu caracter personal către alţi operatori de date[18]; dreptul la portabilitatea datelor personale este stratificat în câteva prerogative specifice, care pot fi decelate secvenţial, pe anumite paliere. Astfel, după cum s-a evidenţiat în literatura de specialitate[19], dreptul de a primi datele într-un format portabil aparţine titularului, care poate conserva informaţiile pentru uz personal ori le poate transmite altui operator, dreptul de a obţine permutarea datelor exercitându-se fără ca operatorul precedent să aibă un drept de opoziţie relativ la exercitarea prerogativelor de portare. După cum s-a opinat, cu just temei, în doctrina de specialitate, în această manieră, „persoana vizată păstrează controlul asupra propriilor date, iar responsabilitatea operatorilor este consolidată. Aceleaşi date pot servi unor scopuri diferite ale prelucrării, în cazul unor servicii distincte, astfel că dreptul la portabilitate încurajează persoanele vizate să îşi recupereze datele şi să le reutilizeze”[20].

Plasat sub o dublă limită, care îi permite prerogativei portabilităţii să depăşească rolul de „Cenuşăreasă” al reglementării din cuprinsul Regulamentului General, domeniul de aplicare al portabilităţii datelor cu caracter personal este restrâns, mai întâi, din punct de vedere subiectiv şi, simultan, obiectiv, întrucât portabilitatea priveşte datele cu caracter personal ce aparţin persoanei vizate; pot fi portate datele furnizate voluntar de către persoana vizată operatorului, în baza unui consimţământ de tip *opting-in,* care ulterior poate fi retractat, în principiu, în orice moment (cu excepţia datelor care rămân în continuare necesare pentru executarea obligaţiilor rezultate dintr-un contract aflat în curs de executare). Responsabilul prelucrării are obligaţia de a se conforma şi de a transmite datele solicitate, putându-se astfel configura arhitectura acestui drept de a obţine portarea datelor cu caracter personal, ca expresie a prerogativelor persoanei vizate de retractare a propriului consimţământ la prelucrare. În alţi termeni, dreptul de retractare a consimţământului la prelucrarea datelor personale, care ar fi de esenţa prelucrării bazate pe consimţământ în economia prevederilor RGDP, încapsulează inclusiv această prerogativă de a solicita şi de a obţine, pe cât posibil, recuperarea setului de date cu caracter personal (transmise, în mod activ şi conştient, operatorului, precum şi datele ce rezultă din activităţile subiectului), într-un format care ar permite reutilizarea acestora.

Sub aspectul consecinţelor exercitării acestui drept la portabilitate, posterior stabilirii dreptului persoanei vizate de a prelua controlul asupra datelor care o privesc, întrebarea evidentă (cu răspunsuri mai puţin evidente) se referă la conturarea unor repere clare cu privire la ceea ce presupune exerciţiul efectiv al acestui drept[21]. În temeiul dispoziţiilor art. 20 GDPR, persoana vizată are dreptul

[18] Grupul de lucru „Articolul 29” pentru protecția datelor, „Ghid privind dreptul la portabilitatea datelor”, [Online] la https://www.dataprotection.ro/servlet/View Document?id=1383, accesat 15.11.2021.

[19] C. Jugastru, „Dreptul la portabilitatea datelor”, *loc. cit. supra.*

[20] *Ibidem.*

[21] Înainte de a trece la enunţarea limitărilor existente, ar trebui să remarcăm succint că mecanismul de aplicare al Regulamentului general privind protecția datelor este aşezat pe un trepied al remediilor juridice: neasigurarea portabilității datelor poate conduce la

de a primi datele personale într-un format structurat, utilizat în mod curent şi care poate fi citit automat (răspuns care, după cum am specificat în paragrafele precedente, va fi emis în termen de o lună de la primirea cererii – conform dispoziţiilor art. 12, par. (3) RGDP). Formularea pentru care a optat legiuitorul european în textul art. 20 din Regulamentul General privind protecţia datelor cu caracter personal implică faptul că nu este suficient ca persoana vizată să poată extrage individual unele din aceste date personale[22], strict secvenţial; mai degrabă, controlorul trebuie să furnizeze un set structurat de date, care să prezinte atributele de a putea fi considerat, din punct de vedere tehnic, un set portabil de date personale[23]. În ipotezele în care este fezabil din punct de vedere tehnic, persoana vizată poate solicita operatorului să transmită respectivele date într-o manieră directă, non-intermediată, altui operator, specificându-se în literatura de specialitate[24] că atât recepţia, cât şi transmiterea datelor cu caracter personal pot fi solicitate în orice moment al prelucrării datelor (anterior eventualei anonimizări), fiind, în principiu, exercitate cu titlu gratuit (cu excepţia unor costuri rezonabile care pot fi percepute pentru onorarea unor cereri repetitive de acces / de portare formulate de respectivul titular la intervale scurte de timp).

Pe marginea definirii noţiunii de *interoperabilitate* în acest context, al portării datelor cu caracter personal, în doctrina de specialitate s-a subliniat[25] că regula

angajarea răspunderii civile a operatorului și, pe un palier secund, la un drept la despăgubiri în temeiul art. 82 RGDP, respectiv la impunerea de sancțiuni care intră în competențele Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

[22] A se vedea P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez, *op. cit.*, p. 197; autorii citați subliniază că: *"In sum, it becomes very clear that the right to data portability – in the final version of the GDPR – is composed of three different rights: 1) the right to receive (without hindrance from the data controller) data concerning data subject which he/she has provided; 2) the right to transmit (without hindrance from the data controller) those data to another controller; and 3) the right to have the personal data transmitted directly from one controller to another. While rights 1) and 2) can be exercised in any case where the processing is based on consent or on a contract and when the processing is carried out by automated means, right 3) needs one more condition: "where technically feasible". The format in which data should be transferred is "structured, commonly used and machine-readable", but the reference to "technical feasibility" is not related to the structured and machine-readable format, but to the "interoperability" of systems, as outlined in recital 68 of GDPR."*

[23] D. Gill, W. Kerber, „Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data", *loc. cit. supra.*

[24] E. Bozdag, „Data Portability Under GDPR: Technical Challenges", *loc. cit. supra.*

[25] P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez, *op. cit.*, p. 197; autorii citați evidențiază că: "*As regards interoperability of systems, the European Commission has defined it as "the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems". Interoperability does not mean "compatibility", as recital 68 clarifies. At the same time, WP29 in its recent guidelines highlights that the determination of the interoperable formats is sector-specific."*

implică faptul că există formate de date utilizate în mod obişnuit pentru respectivele tipuri de date. Autorii care s-au ocupat de subiect au reţinut că, deşi acest aspect se poate dovedi adevărat pentru o multitudine de ipoteze, cu siguranţă, nu este aplicabil tuturor tipurilor de date personale; ar putea fi nominalizate, pentru exemplificare, reacţiile de tip *like* de pe o platformă de socializare sau datele captate de funcţiile *smart* ale unor dispozitive cu conţinut digital incorporat, în cazul cărora formatul utilizat pentru colectarea datelor personale ar putea fi incompatibil cu cel al altor dispozitive, în eventualitatea primirii unei cereri de portare. S-a susţinut mai degrabă că, într-o astfel de situaţie, operatorul poate îndeplini cerinţa de portabilitate furnizând datele în formatul utilizat la momentul prelucrării. De asemenea, nu este clar, invariabil, în practică despre cum urmează să fie determinat standardul de fezabilitate tehnică al unui transfer direct de date cu caracter personal, prin prisma faptului că un mecanism care este fezabil din punct de vedere tehnic pentru giganţi ai prelucrării datelor cu caracter personal poate fi dificil de implementat pentru controlorii de mai mici dimensiuni (de exemplu, clinici medicale de dimensiunii medii ca cifre de afaceri, care ar procesa date sensibile cu privire la care vor primi cereri de portare) şi care „trebuie să se bazeze pe un *software* dezvoltat şi susţinut de terţi."[26] – (tr. n., J. G.).

2. Remarci legate de interferenţele dintre reglementarea dreptului la portabilitatea datelor conform prevederilor art. 20 RGDP şi dispoziţiilor Directivei 2019/770 privind furnizarea de conţinut digital şi servicii digitale

Binar în disjungerea pe care o operează între etapa executării contractului şi momentul începând cu care este exercitabil dreptul la portabilitatea datelor, sistemul de reglementare existent în cuprinsul Directivei 2019/770 privind anumite aspecte referitoare la contractele de furnizare de conţinut digital este centrat pe două dispoziţii privind portabilitatea conţinutului digital, regulile propuse distanţându-se de cele enunţate în textul art. 20 RGDP sub două aspecte semnificative, care pot fi decelate astfel: (1) în principiu, dreptul la portabilitatea conţinutului digital se aplică numai după rezilierea unui contract B2C pentru furnizarea de conţinut digital sau, altfel spus, la încetarea acestuia, neexistând pe parcurs (în etapa derulării raporturilor contractuale B2C) în privinţa conţinutului digital (etapă în care ar putea fi, însă, exercitat dreptul la portarea nu a întregului conţinut digital disponibil, ci a datelor personale în temeiul art. 20 RGDP); (2) dreptul la portabilitate nu se limitează la datele cu caracter personal, ci se extinde, în textul Directivei 2019/770, asupra tuturor tipurilor de conţinut digital generate inclusiv prin înglobarea unor date cu caracter personal ale utilizatorilor.

Escamotând problematicile privitoare la valabilitatea clauzelor contractuale de amenajare a întinderii / sferei materiale a dreptului la portabilitatea conţinutului

[26] *Ibidem.*

digital[27], am putea reţine că Directiva adoptată în 2019 indică posibilitatea ca un contract B2C privind furnizarea de conţinut digital să prevadă obligaţia corelativă a consumatorului, fie de a achita un preţ, care ar reprezenta contravaloarea serviciului digital furnizat, fie să ofere în mod asertiv contraprestaţii, altele decât sumele de bani, sub forma furnizării de date cu caracter personal. Condiţia prealabilă a furnizării „active" de date a fost criticată ca fiind vagă, insuficient de precisă, pentru a configura un regim juridic coerent[28], şi anume din perspectiva faptului că datele care sunt colectate *implicit* de la consumator pe durata prestării unui serviciu digital vor prezenta adesea mai mult interes pentru furnizor decât datele pe care consumatorul le-a oferit în mod activ. Aserţiunea rămâne valabilă chiar şi în cazul în care consumatorul furnizează în mod activ date cu caracter personal, întrucât aceste date nu vor fi considerate a reprezenta o veritabilă contraprestaţie, dacă datele sunt strict necesare pentru executarea contractului sau pentru îndeplinirea cerinţelor legale, atât timp cât furnizorul nu utilizează datele pentru alte scopuri, în special cele comerciale sau scopuri de *marketing* personalizat. Pe cale de consecinţă, pot exista situaţii practice în care furnizarea de date personale cu ocazia prestării unui serviciu digital nu este considerată o contraprestaţie activă din partea consumatorului. Cu toate acestea, în practică, această exceptare va intra rareori în joc, deoarece datele despre consumatori sunt utilizate în mod regulat, ulterior, de către furnizorii serviciilor digitale în alte scopuri decât executarea efectivă a contractului, discuţia glisând în perimetrul *advertising*-ului personalizat, ceea ce transformă respectivele date într-o contraprestaţie furnizată de consumator, declanşând aplicabilitatea dispoziţiilor

[27] După cum s-a observat în doctrina de specialitate, *"The distinction between **data observed** on the data subject and **data created** by the data controller is crucial to define the scope of the right to portability, but it is also one of the most difficult to make and requires case-by-case examination."* (s.n. – J.G.): M. Borghi, *op. cit.*, p. 9. Dispozițiile Directivei 2019/770 se aplică, sub aspectul sferei materiale de incidență, contractelor între profesioniști și consumatori pentru furnizarea de conținut digital, cum ar fi fișiere video și audio, *software*, stocare în *cloud*, rețele sociale și fișiere de modelare vizuală pentru imprimare 3D, precum și jocuri, servicii e-mail, intermediere *online* de tranzacții și platforme de partajare, iar dispozițiile privind portabilitatea se vor aplica ori de câte ori normele de drept internațional privat indică dreptul contractual al unui stat membru al UE (conform art. 4 și 6 din Regulamentul Roma I), ca fiind incident.

[28] A se vedea A. Metzger, „A Market Model for Personal Data: State of Play Under the New Directive on Digital Content and Digital Services", *loc. cit. supra*; autorul citat subliniază că: *"According to the old paradigm, "free services" were offered to consumers who gave their consent to the processing of their data. Both transactions were seen as being independent of each other. The leading search engines, social media platforms and many "content" providers did not – and still do not – demand for a money consideration from the users. Those services therefore appeared as if they would be gratuitous for the consumer, whereas the service providers earned their revenues on the other side of the market by selling advertisements to business customers. The processing of the data, either based on consent or on the other legal grounds of Article 6 para. 1 General Data Protection Regulation (GDPR), was interpreted as an ancillary unilateral legal act besides the service contract".*

privitoare la portabilitatea datelor. Prevederile Directivei 2019/770, în versiunea finală a acestora, sunt aplicabile indiferent dacă un consumator furnizează datele personale în mod activ sau pasiv, având în vedere că formularea „furnizate în mod activ" din cuprinsul art. 3, alin. (1) şi alin. (2) a fost, în final, abandonată în textul Directivei. Cu toate acestea, rămâne de actualitate remarca potrivit căreia Directiva nu oferă o soluţie clară, specific calibrată pentru datele colectate de la un consumator pasiv; potrivit considerentului (24), este suficient ca datele cu caracter personal să fie „create" prin utilizarea conţinutului digital sau a serviciului digital, astfel încât chiar şi o simplă colecţie de meta-date, cum ar fi informaţiile referitoare la localizarea consumatorului sau istoricul de navigare poate fi suficientă, conform considerentului (25), pentru a reţine existenţa dreptului la portabilitate.

Cerinţa furnizării „active" a datelor prezintă, de asemenea, interes în mod indirect în ceea ce priveşte *software*-ul incorporat sau al produselor cu conţinut digital incorporat, o problematică ce suscită dezbateri suficient de ample în literatura de specialitate. În conformitate cu explicaţiile reţinute în Considerentul (11) al Directivei 2019/770, dispoziţiile privind vânzările *online* se aplică *software*-ului încorporat dacă funcţiile *software*-ului sunt subordonate principalelor funcţionalităţi ale produselor contractate şi funcţionează ca parte integrantă a produsului livrat, distincţie care a fost pe larg criticată în literatura de specialitate[29]. În ceea ce priveşte portabilitatea datelor, miza practică nu ar putea fi escamotată, fiind de reţinut că vânzătorul produsului cu conţinut digital incorporat sau furnizorul *software*-ului încorporat şi operatorul care colectează date prin intermediul *software*-ului încorporat vor fi adesea părţi diferite; de exemplu, în ipotezele în care obiectul derivat al vânzării îl reprezintă un dispozitiv cu funcţii *smart* (cu conţinut digital inclus), vânzătorul nu colectează de regulă datele generate prin utilizarea *software*-ului încorporat, acestea fiind colectate, în schimb, de către furnizorul sistemului de operare al dispozitivului *smart*. Cu toate acestea, dreptul de a prelua date cu caracter personal este activat numai dacă între consumator şi vânzătorul produsului cu conţinut digital incorporat a fost încheiat

[29] *Ibidem*; autorul citat evidenţiază că: *"The language of Article 3 para. 1 sub-para. 2 DCSD-Proposal was at the same time explicit and narrow. It was explicit that personal data or other data could be interpreted as counter-performance of the consumer which provoked the severe criticism of the European Data Protection Supervisor. However, the scope of application was rather narrow with regard to personal data that could qualify as counter-performance. Article 3 para. 1 sub-para. 2 only mentioned "actively provided" data. Recital 14 excluded data automatically generated and collected by cookies and also data "necessary for the digital content to function in conformity with the contract, for example geographical location where necessary for a mobile application to function properly", and data collected "for the sole purpose of meeting legal requirements". These restrictions were criticized both by academics and consumer organisations, a criticism that was finally taken up by the European Parliament which requested a broader inclusion of personal data into the framework of the Directive. The final text of Article 3 para. 1 sub-para. 2 DCSD addresses both concerns. The revised text avoids the words "personal data as counter-performance" to make clear that the European legislature does not encourage a further commercialisation of personal data.12 All the safeguards of the GDPR remain untouched, see Article 3 para. 8 and Recital 38 DCSD."*

un contract B2C, ceea ce ar implica ulterior că ar fi necesar să ţinem cont de existenţa şi arhitectura acestei relaţii tripartite, atunci când elaborăm sfera de aplicare a dreptului la portabilitatea datelor[30].

Pe celălalt versant al discuţiei, conform dispoziţiilor art. 9 din Directiva 2019/770, privind integrarea incorectă a conţinutului digital sau a serviciului digital, „*Orice neconformitate cauzată de integrarea incorectă a conţinutului digital sau a serviciului digital în mediul digital al consumatorului este considerată ca reprezentând o neconformitate a conţinutului digital"* dacă: (a) respectivul conţinut digital sau serviciu digital a fost integrat de către vânzătorul profesionist ori de subcontractanţi pentru care acesta răspunde; ori (b) conţinutul digital a fost destinat să fie integrat de consumator, iar integrarea incorectă s-a datorat unor deficienţe în instrucţiunile de integrare furnizate acestuia. După cum rezultă din paragrafele Considerentului (48) al Directivei 2019/770, nerespectarea obligaţiilor prevăzute în Regulamentul (UE) 2016/679 ar putea, în acelaşi timp, să implice *per se* o neconformitate a conţinutului digital sau a serviciului digital, făcându-l impropriu scopului său şi, prin urmare, să constituie o neconformitate raportat la cerinţele obiective de conformitate, care impun ca serviciul digital să fie adecvat scopurilor tipice pentru care ar fi utilizat în mod uzual conţinutul digital sau serviciile digitale de acelaşi tip[31]. În fine, ar putea exista cazuri în care nerespectarea de către profesionistul vânzător a obligaţiilor care îi revin în temeiul Regulamentului (UE) 2016/679 poate constitui, de asemenea, o carenţă de conformitate a conţinutului digital sau a serviciului digital cu cerinţa obiectivă de conformitate care impune ca respectivul conţinut digital sau serviciul digital să aibă caracteristicile normale, tipice pentru conţinutul digital sau pentru serviciile digitale de acelaşi tip şi la care consumatorul se poate aştepta în mod rezonabil. De exemplu, în cazul în care profesionistul furnizor al unei aplicaţii de cumpărături *online* nu antamează măsurile prevăzute în Regulamentul (UE) 2016/679 pentru securitatea prelucrării datelor cu caracter personal ale consumatorului şi, în consecinţă, informaţiile privind cardul de credit / debit al consumatorului sunt expuse la programe *malware* sau *spyware*, aspect care ar putea constitui, de asemenea, o neconformitate a conţinutului digital sau a serviciului digital în sensul Directivei 2019/770, întrucât consumatorul s-ar aştepta, în mod rezonabil, ca o astfel de aplicaţie să prezinte *by design* caracteristici care să împiedice divulgarea detaliilor privind plăţile efectuate. În cazul în care aspectele care conduc la o nerespectare a cerinţelor prevăzute în Regulamentul (UE) 2016/679 constituie, de asemenea, o neconformitate a conţinutului digital sau a serviciului digital cu cerinţele subiective

[30] H. Vrabec, „The Failure of Control Rights in the Big Data Era – Does a Holistic Approach Offer a Solution?", *loc. cit. supra.*

[31] Astfel s-ar întâmpla, de exemplu, în cazul în care profesionistul care comercializează un *software* de criptare a datelor nu reușește să pună în aplicare măsurile adecvate impuse de Regulamentul (UE) 2016/679 pentru a se asigura că datele cu caracter personal din momentul conceperii nu sunt divulgate unor destinatari neautorizați, ceea ce ar face ca *software*-ul de criptare să nu fie adecvat scopului său, care este transferul în condiții de siguranță al datelor de către consumator către destinatarul preconizat.

sau obiective de conformitate prevăzute în Directiva 2019/770, consumatorul ar urma să beneficieze de dreptul la măsurile corective în caz de neconformitate prevăzute de această directivă, cu excepţia cazului în care contractul este anulabil în temeiul dispoziţiilor de drept intern.

Sunt relevante, de asemenea, dispoziţiile art. 16, îndeosebi alin. 3, 4 şi 5 din Directiva 2019/770, privind obligaţiile vânzătorului / furnizorului în cazul încetării / terminării contractului, conform cărora „Furnizorul conţinutului digital ori al serviciului digital se va abţine pentru viitor, posterior încetării raporturilor contractuale cu consumatorul, de la utilizarea oricărui alt conţinut în afara datelor cu caracter personal care au fost furnizate sau create de consumator la utilizarea conţinutului digital sau a serviciului digital furnizat[32].

Cu excepţia situaţiilor menţionate la alin. (3), lit. (a), (b) sau (c), din alin. (4) al art. 16 din Directiva 2019/770 rezultă că furnizorul conţinutului digital ori al serviciului digital „va pune la dispoziţia consumatorului, la cererea acestuia, orice conţinut care nu reprezintă date cu caracter personal, care a fost furnizat sau creat de către consumator în momentul utilizării conţinutului digital sau a serviciului digital", consumatorul având dreptul de a recupera respectivul conţinut digital într-o manieră gratuită, non-oneroasă, fără costuri suplimentare / fără contraprestaţie şi fără impedimente din partea furnizorului conţinutului digital, într-un termen rezonabil şi într-un format utilizat în mod curent, care să poată fi citit automat într-un mediu digital. Din paragraful (5) al art. 16 din Directiva 2019/770 rezultă că furnizorul conţinutului digital ori al serviciului digital poate împiedica orice utilizare ulterioară a conţinutului digital sau a serviciului digital de către consumator, „în special prin oprirea accesului consumatorului la conţinutul digital sau la serviciul digital sau prin dezactivarea contului de utilizator al consumatorului", fără a aduce atingere prevederilor alin. (4) privitoare la portarea conţinutului generat.

Se menţionează în literatura de specialitate că, în contextul datelor furnizate, datele derivate (datele deduse) nu intră în sfera dreptului la portabilitate, „dar rămâne posibil pentru utilizator să solicite operatorului de date să îi comunice dacă datele sale au făcut sau nu obiectul prelucrării, iar în caz afirmativ, care au fost scopurile prelucrării"[33]. Ca principiu generic, nu fac obiectul portabilităţii datele care sunt prelucrate pe alte temeiuri decât cele menţionate de art. 20, alin. (1), lit. a), a căror prelucrare se fondează pe alte temeiuri decât consimţământul persoanei vizate ori nu sunt date personale necesare pentru executarea contractului. De asemenea, în principiu, portabilitatea nu presupune ştergerea datelor, întrucât, de exemplu, „nu presupune ştergerea datelor furnizate de persoana vizată în vederea

[32] Sunt exceptate cazurile în care acest conținut: „(a) nu are vreo utilitate în afara contextului utilizării conținutului digital sau al serviciului digital furnizat de profesionist; (b) are legătură doar cu activitatea consumatorului atunci când folosește conținutul digital sau serviciul digital furnizat de vânzător; (c) a fost agregat cu alte date de către profesionist și nu poate fi dezagregat sau poate fi dezagregat numai cu eforturi disproporționate; (d) a fost generat în comun de către consumator și alte persoane vizate, iar alți consumatori pot continua să utilizeze conținutul." (art. 16 DCDSD).

[33] C. Jugastru, „Dreptul la portabilitatea datelor", *loc. cit. supra.*

executării unui contract, în măsura în care datele respective sunt utile pentru executarea contractului"[34]. Se cuvine menţionat că portarea nu creează obligaţia responsabilului de a conserva datele pe o perioadă mai îndelungată decât cea prevăzută iniţial, în directă corelare cu scopurile prelucrării. Fezabilitatea tehnică a transmiterii de la un operator la altul, sub controlul persoanei vizate, va trebui evaluată în practică plecând de la circumstanţele fiecărui caz în parte. Considerentul (68) RGDP clarifică în continuare limitele a ceea ce este acceptabil din „punct de vedere tehnic", indicând faptul că „nu ar trebui să genereze o obligaţie pentru operatori de a adopta sau de a menţine sisteme de prelucrare care să fie compatibile din punct de vedere tehnic" în ideea facilitării portării datelor cu caracter personal, astfel încât operatorilor de date personale nu le incumbă, în baza dispoziţiilor Regulamentului General, vreo obligaţie de adaptare a mecanismelor tehnice utilizate în scopul facilitării portării acestor date. În alţi termeni, merită accentuată aserţiunea conform căreia operatorilor nu le revine obligaţia de a adopta sau de a menţine sisteme de prelucrare care să fie compatibile din punct de vedere tehnic, prin prisma rezolvării eventualelor cereri de portare a datelor colectate şi prelucrate.

În pofida faptului că setul de meta-norme descris în art. 20 RGDP în materia portabilităţii datelor personale nu include obligaţia operatorilor de a compatibiliza programele *software* folosite, este de aşteptat ca operatorii să transmită date cu caracter personal într-un format interoperabil, cu toate că RGDP nu stabileşte obligaţii pentru alţi operatori în vederea sprijinirii acestor formate. Prin urmare, transmiterea directă de la un operator la altul ar putea apărea atunci când comunicarea între cele două sisteme este posibilă, într-un mod securizat, şi în cazul în care sistemul de primire a datelor are capacitatea, din punct de vedere tehnic, de a primi datele transmise. În situaţia în care obstacolele tehnice fac imposibilă transmiterea directă, operatorul trebuie să explice aceste impedimente persoanelor vizate, întrucât, în caz contrar, decizia sa va fi similară, în efectul său, unui refuz[35] de a lua măsuri ca urmare a unei cereri a persoanei vizate conform dispoziţiilor art. 12 par. (4) din Regulamentul General.

3. Paradigmatică, dar incertă: preeminenţa temeiurilor extrase din prevederile RGDP privind portabilitatea datelor

În literatura de specialitate s-a ridicat problema de a stabili în ce măsură ar putea fi reţinută (in)existenţa unei preeminenţe a prevederilor RGDP privitoare la portabilitate, dacă un drept la portabilitate ia naştere, pentru consumator, atât în temeiul art. 20 RGDP, cât şi în temeiul prevederilor Directivei 2019/770 privind conformitatea conţinutului digital, în eforturile doctrinare de a răspunde interogaţiilor în ce măsură consumatorul poate alege pe ce regulă se bazează solicitarea sa de portare a datelor – sau chiar dacă îşi poate fonda cererea de portare pe ambele

[34] *Ibidem.*

[35] G. Nicholas, „Taking It With You: Platform Barriers to Entry and the Limits of Data Portability", *loc. cit. supra.*

seturi de norme speciale, cumulând cele două mecanisme juridice privind portarea datelor cu caracter personal. Considerentele 37, 38 şi 39, precum şi dispoziţiile Art. 3, par. (6) şi (8) din Directiva 2019/770 clarifică faptul că regulile propuse în cadrul directivei nu aduc atingere normelor Regulamentului General privind protecţia datelor, subliniindu-se în doctrina de specialitate că ar fi logic ca niciuna dintre regulile de portabilitate să nu aibă prioritate faţă de cealaltă, deoarece dispoziţiile din Regulamentul general, respectiv din Directiva 2019/770 în materie de portabilitate prezintă atât particularităţi, cât şi o suprapunere semnificativă, rămânând să ţintească obiective de legiferare distincte. Dacă exigenţele legale intrinseci şi prerechizitele exogene (rezilierea unui contract B2C pentru furnizarea de conţinut digital sau încetarea acestui contract) pentru admisibilitatea unei cereri a consumatorului de portare a datelor personale sunt îndeplinite în temeiul dispoziţiilor Directivei 2019/770, consumatorul nu va trebui să recurgă suplimentar la prevederile RGDP, reciproca fiind de asemenea valabilă, prin prisma faptului că cele două reglementări nu se exclud (chiar dacă, parţial, sfera lor materială şi personală de executare rămâne a fi diferită). Pe de altă parte, în cazul în care unele dintre cerinţele aplicabile solicitării consumatorului de portare a datelor vor fi îndeplinite numai în temeiul art. 20 RGDP (transmiterea către un alt operator de date), iar alte cerinţe vor fi îndeplinite numai în cadrul remediilor neconformităţii descrise în prevederile Directivei 2019/770 (privind portabilitatea conţinutului digital, care încorporează parţial date personale), este util pentru consumator să asocieze şi o cerere distinctă privind portarea datelor personale fondată pe prevederile art. 20 RGDP. Mecanismul portării datelor personale în temeiul art. 20 RGDP rămâne, în continuare, util (şi chiar indispensabil) pe durata derulării raporturilor contractuale B2C în privinţa conţinutului digital, când niciuna dintre părţi nu s-a prevalat de dreptul de a solicita rezilierea contractului, etapă în care ar putea fi exercitat dreptul la portarea nu a întregului conţinut digital disponibil, ci a datelor personale colectate şi prelucrate în temeiul consimţământului utilizatorului.

Existenţa unui contract B2C (de furnizare a conţinutului digital) în derulare se numără printre prerechizitele aplicării dreptului la portabilitate în temeiul prevederilor Directivei 2019/770, fără a o regăsi, însă, printre condiţiile indispensabile exercitării dreptului la portabilitate în temeiul art. 20 RGDP, ceea ce se coagulează ca o diferenţă majoră între sfera de aplicare ale acestui drept în economia dispoziţiilor DCSD şi, după caz, ale RGDP; cu toate acestea, întrebarea centrală se referă la a stabili dacă o situaţie în care consumatorul utilizează un serviciu digital fără a fi contractat în mod expres, de exemplu, în cazul în care iniţiază o căutare utilizând un motor de căutare *online*, prilej cu care furnizorii de servicii asociate utilizării motoarelor de căutare *web* colectează datele personale ale consumatorului[36], trebuie sau nu calificate drept un veritabil contract B2C, aspect care nu a fost reglementat explicit în Directiva 2019/770, în contextul în care art. 3 reţine că Directiva privind contractele de furnizare a conţinutului digital „nu

[36] A se vedea A. Metzger, *op. cit.*, p. 4.

afectează libertatea statelor membre de a reglementa aspecte ale dreptului general al contractelor, precum regulile privind formarea, valabilitatea, nulitatea sau efectele contractelor", urmând ca, la nivelul dispoziţiilor dreptului intern, să se tranşeze inclusiv răspunsul la interogaţiile ridicate pe acest palier, al (in)existenţei unui veritabil contract între utilizatorul serviciului web şi operatorul de date cu caracter personal.

Distincţia dintre consimţământul (in)valid şi cazurile de formare veritabilă a contractului privind furnizarea de conţinut digital sau servicii digitale în temeiul prevederilor Directivei 2019/770 prezintă, de asemenea, relevanţă[37] pentru gestionarea corelaţiilor cu interdicţia prezentă în textul art. 7, alin. (4) RGDP, din perspectiva „cuplării" consimţământului la formarea contractului propriu-zis (de furnizare a conţinutului digital ori a serviciilor digitale, în acest caz) şi, pe de altă parte, a consimţământului la prelucrarea datelor cu caracter personal, inclusiv în contextul executării respectivului contract (un temei juridic *per se* al prelucrării datelor personale)[38]. „Decuplarea" celor două consimţăminte (la prelucrarea datelor personale şi, respectiv, la formarea contractului B2C) este elementară în economia noţiunii de „consimţământ liber furnizat" prin prisma prevederilor art. 7, par. (4) RGDP, din care rezultă că va fi folosit drept criteriu decisiv în evaluarea libertăţii de a consimţi la prelucrarea datelor cu caracter personal în contextul contractării B2C. În literatura de specialitate[39], a fost remarcată utilizarea sintagmei (edulcorate) „se ţine seama cât mai mult de faptul că, printre altele, executarea unui contract (...)"[40], ceea ce imprimă un anumit grad de flexibilitate în utilizarea acestui criteriu, în pofida „vestimentaţiei" de aparentă interdicţie imperativă a oricărei combinaţii de tipul asocierii consimţământului la prelucrarea datelor personale (i) şi a acordului la formarea şi executarea contractului (substanţial) (ii); strict tehnic, chiar şi în ipotezele în care ar rezulta că acordul utilizatorului la colectarea şi prelucrarea datelor sale personale ar fi invalid prin prisma dispoziţiilor art. 7, par. (4) RGDP, din pricina condiţionării acestui acord într-o manieră incompatibilă cu caracterul liber exprimat, contractul de furnizare a conţinutului digital ar rămâne valabil format, fiind incidente, în acest caz, prevederile Directivei 2019/770, inclusiv cu privire la portabilitatea datelor la finele raporturilor contractuale.

[37] *Idem*, p. 7.

[38] Potrivit prevederilor art. 7, par. (4) RGDP, „(4) Atunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract."

[39] A se vedea A. Metzger, *op. cit.*, p. 7.

[40] *Idem*, p. 8; autorul citat evidențiază, în termeni tranșanți, că, în cele din urmă, reprezintă o chestiune de interpretare a (clauzelor neclare ale) contractului: *"If and to what extent a consumer has an obligation to provide personal data under a contract and to give its consent in the processing of that data, or whether the processing of data is a mere side-effect of the contract, is first and foremost a question of contract interpretation."*

Aceleaşi principii rămân incidente şi în cazul retragerii ulterioare a consimţământului persoanei vizate la prelucrarea datelor personale, potrivit art. 7, par. (3) RGDP, persoana vizată putându-şi retrage consimţământul la prelucrarea datelor personale în orice moment (fără ca retragerea consimţământului să afecteze legalitatea prelucrării bazate pe consimţământ anterior retragerii acestuia), în timp ce, dimpotrivă, retragerea consimţământului care a generat formarea contractului de furnizare a unor servicii digitale nu poate avea loc într-o manieră unilaterală, ca regulă generală fiind aplicabil *mutuus dissensus*, chiar dacă rămâne posibilă invocarea carenţelor de neconformitate pentru a obţine rezoluţiunea / rezilierea judiciară a contractului; ceea ce rămâne de decelat în temeiul art. 7, alin. (3) RGDP este răspunsul la interogaţia cu privire la consecinţele retragerii acordului utilizatorului la prelucrarea datelor sale cu caracter personal, prelucrarea ulterioară a acestora rămânând posibilă că fondată pe necesitatea executării contractului, fără a mai avea ca fundament consimţământul utilizatorului.

Eboşa astfel trasată trebuie întregită cu trimiterile la prevederile art. 3, alin. (1), teza a II-a din Directiva 2019/770, care menţionează că dispoziţiile Directivei devin inaplicabile în cazul în care datele cu caracter personal sunt prelucrate exclusiv de comerciant în scopul furnizării de conţinut digital sau servicii digitale sau pentru a permite comerciantului să respecte cerinţele legale la care este supus în această materie, iar comerciantul nu procesează aceste date personale în orice alt scop. Pe cale de consecinţă, aplicarea dispoziţiilor Directivei 2019/770 nu poate fi reţinută în ipotezele în care prelucrarea datelor personale se bazează pe art. 6, alin. (1), lit. b) şi c) din RGDP, precum în cazul, de exemplu, în care un serviciu de navigaţie rutieră prelucrează datele de locaţie cu unicul scop de a recomanda traseul adecvat către consumator; este fastidios de amintit că, în aceste cazuri, prelucrarea datelor personale trebuie să rămână cantonată între limitele descrise de scopurile menţionate, în caz contrar, fiind aplicabil setul de norme din cuprinsul Directivei 2019/770 privind furnizarea de conţinut digital[41].

4. Remarci concluzive

Erodat, în practică, de eventuala incompatibilitate tehnică între formatele de portare utilizate, mecanismul portabilităţii datelor cu caracter personal prezintă o utilitate indeniabilă, inclusiv în perimetrul executării contractelor de furnizare a conţinutului digital şi de prestare a serviciilor digitale. Domeniul de aplicare al portabilităţii datelor cu caracter personal este restrâns, mai întâi, din punct de vedere subiectiv şi, simultan, obiectiv, întrucât portabilitatea priveşte datele cu

[41] *Ibidem*; autorul citat reţine că: *"Regrettably, the DCSD does not provide a clear-cut rule for cases in which the processing of data is based on Article 6 para. 1 lit. f) GDPR, i.e. is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party", or on other statutory grounds, Article 6 para. 1 lit. e), para. 2 GDPR. The issue is of growing interest, especially if one shares the criticism of consent as the commonly used basis of data processing.42 Lengthy "data policies" and "privacy statements" do indeed, as put forward by the critics, prevent the consumer from taking an informed decision".*

caracter personal ce aparţin persoanei vizate; pot fi portate datele furnizate voluntar de către persoana vizată operatorului, în baza unui consimţământ de tip *opting-in*, care ulterior poate fi retractat, în principiu, în orice moment (cu excepţia datelor care rămân în continuare necesare pentru executarea obligaţiilor rezultate dintr-un contract aflat în curs de executare). Responsabilul prelucrării are obligaţia de a se conforma şi de a transmite datele solicitate, putându-se astfel configura arhitectura acestui drept de a obţine portarea datelor cu caracter personal, ca expresie a prerogativelor persoanei vizate de retractare a propriului consimţământ la prelucrare.

La fel cum gambitul damei poate fi acceptat sau poate fi refuzat de către jucător, „gambitul" propus de utilizator prin angajarea portabilităţii datelor sale personale în temeiul prevederilor Directivei 2019/770 anterior încetării contractului prin reziliere / anterior desfiinţării raporturilor contractuale poate fi refuzat de operatorul de date (furnizorul de servicii digitale), în timp ce o eventuală cerere de portare fondată pe prevederile art. 20 RGDP nu ar putea fi contracarată niciun moment de către operatorul de date, nefiind permisă plasarea de obstacole nerezonabile în exercitarea acestor prerogative ale persoanei vizate. Spre deosebire de gambitul regelui, în gambitul damei, pionul este fie recâştigat, fie va fi menţinut lângă piesele negre; pentru utilizatorul serviciilor digitale, invocarea prevederilor art. 20 RGDP rămâne utilă dacă doreşte să obţină transmutarea datelor cu caracter personal într-un format portabil până la momentul rezilierii contractului de furnizare a conţinutului digital / serviciilor digitale, moment de la care s-ar putea prevala de dispoziţiile Directivei 2019/770 pentru a obţine portarea datelor / fişierelor încărcate ori create cu ajutorul conţinutului digital contractat, incluzând eventualele date cu caracter personal astfel utilizate. Următoarele observaţii concluzive pot fi formulate, pe marginea consideraţiilor din secţiunile precedente:

(a) portabilitatea datelor se bifurcă în dreptul unei persoane fizice „de a primi datele cu caracter personal care o privesc şi pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent şi care poate fi citit automat" (i) şi, pe celălalt versant, în dreptul de a transmite aceste date altui operator, fără obstacole nejustificate din partea operatorului căruia i-au fost furnizate datele cu caracter personal (ii), fiind, din start, excluse din sfera materială de incidenţă a acestui drept datele anonimizate sau datele care nu privesc utilizatorul care solicită accesul la datele sale;

(b) datele pseudonimizate, care, prin definiţie, pot fi folosite pentru a identifica utilizatorul, chiar dacă identificarea se face cu ajutorul unor chei de decriptare, rămân să facă obiectul dreptului la portarea datelor, pseudonimizarea nereprezentând *per se* un obstacol în calea exercitării acestor prerogative;

(c) în ipotezele în care este fezabil din punct de vedere tehnic, persoana vizată poate solicita operatorului să transmită respectivele date într-o manieră directă, non-intermediată, altui operator, astfel încât atât recepţia, cât şi transmiterea datelor cu caracter personal pot fi solicitate în orice moment al prelucrării datelor (anterior eventualei anonimizări), fiind, în principiu, exercitate cu titlu gratuit, cu

excepţia perceperii unor costuri rezonabile pentru onorarea unor cereri repetitive de acces / de portare;

(d) clivajul semnalat între regimul portabilităţii datelor personale în temeiul dispoziţiilor art. 20 RGDP şi regimul portabilităţii conţinutului digital reglementat de prevederile Directivei 2019/770 este adâncit de faptul că, în principiu, dreptul la portabilitatea conţinutului digital se aplică numai după rezilierea unui contract B2C pentru furnizarea de conţinut digital sau, altfel spus, la încetarea acestuia, neexistând pe parcurs (în etapa derulării raporturilor contractuale B2C) în privinţa conţinutului digital (etapă în care ar putea fi, însă, exercitat dreptul la portarea nu a întregului conţinut digital disponibil, ci a datelor personale în temeiul art. 20 RGDP);

(e) dreptul la portabilitatea conţinutului digital nu se limitează la datele cu caracter personal încorporate în conţinutul digital propriu-zis, ci se extinde, în textul Directivei 2019/770, asupra tuturor tipurilor de conţinut digital generate / create inclusiv prin înglobarea unor date cu caracter personal ale utilizatorilor;

(f) obligaţia utilizatorului de a furniza date cu caracter personal ar putea ridica probleme de calificare drept contraprestaţie a consumatorului, în sensul unui raport contractual sinalagmatic, aspect amintit mai degrabă aluziv, însă netranşat expres în cuprinsul Directivei 2019/770 privind contractele de furnizare a conţinutului digital; în principiu, revine legiuitorului naţional tranşarea acestei problematici în legătură cu consecinţele unei posibile neexecutări contractuale, îndeosebi în perimetrul situaţiilor în care s-ar ridica problema de a stabili în ce măsură refuzul consumatorului de a furniza datele sale personale ar putea justifica un refuz similar al profesionistului de a furniza conţinutul digital şi în ce măsură ar putea justifica o solicitare de reziliere a contractului de furnizare a serviciilor digitale.

Referinţe

Aertgeerts, P., *Shaping Fundamental Rights: The Right to Data Portability, the EU Legislator and the Normative Foundations of the Fundamental Right to Data Protection* (November 6, 2019)

Alberini, A.; Benhamou, Y., *Data Portability and Interoperability: An Issue that Needs to Be Anticipated in Today's It-Driven World* (August 1, 2017), https://dx.doi.org/10.2139/ssrn.3038877

Araújo Souto, G., *Data Portability: a Necessary Right for Users and Competitors of Digital Platforms* (October 12, 2018), https://dx.doi.org/10.2139/ssrn.3293056

Banda, C., *Enforcing Data Portability in the Context of EU Competition Law and the GDPR*, MIPLC Master Thesis Series 2017

Belo, J.; Macedo Alves, P., *The Right to Data Portability: An In-Depth Look*, Journal of Data Protection and Privacy, Vol. 2, nr. 1/2018

Borghi, M., *Data Portability and Regulation of Digital Markets*, CIPPM / Jean Monnet Working Papers, Bournemouth University, 2019, https://dx.doi.org/10.2139/ ssrn.3617792

Bozdag, E., *Data Portability Under GDPR: Technical Challenges* (January 28, 2018), https://dx.doi.org/10.2139/ssrn.3111866

De Hert, P.; Papakonstantinou, V.; Malgieri, G.; Beslay, L.; Sanchez, I., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, Computer Law & Security Review, 2018

De Streel, A.; Kraemer, J.; Senellart, P., *Making Data Portability More Effective for the Digital Economy* (June 14, 2021), https://dx.doi.org/10.2139/ssrn.3866495

Gill, D.; Kerber, W., *Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data* (October 11, 2020), https://dx.doi.org/10.2139/ssrn.3715357

Graef, I., *The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation*, Competition Policy International, Antitrust Chronicle November 2020 (II)

Graef, I.; Husovec, M.; van den Boom, J., *Spill-Overs in Data Governance: The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes*, TILEC Discussion Paper No. DP 2019-005, 2019, https://dx.doi.org/10.2139/ssrn.3369509

Graef, I.; Clifford, D.; Valcke, P., *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law,* International Data Privacy Law, vol. 8, nr. 3/2018

Graef, I.; Husovec, M.; Purtova, N., *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, German Law Journal, vol. 19, nr. 6/2018, pp. 1359-1398, Tilburg Law School Research Paper No. 2017/22, https://dx.doi.org/10.2139/ssrn.3071875

Hurwitz, J., *Digital Duty to Deal, Data Portability, and Interoperability*, The Global Antitrust Institute Report on the Digital Economy 28, 2020, https://dx.doi.org/10.2139/ssrn.3733744

Jugastru, C., *Dreptul la portabilitatea datelor,* Revista Universul Juridic, disponibil la adresa http://revista.universuljuridic.ro/dreptul-la-portabilitatea-datelor/, on-line

Ke, T.; Sudhir, K., *Privacy Rights and Data Security: GDPR and Personal Data Driven Markets* (July 5, 2020), https://dx.doi.org/10.2139/ssrn.3643979

Kraemer, J., *Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations*, Journal of Competition Law & Economics, 2020

Leistner, M., *The Existing European IP Rights System and the Data Economy – An Overview With Particular Focus on Data Access and Portability*, în J. Drexl (ed.), „Data access, Consumer Protection and Public Welfare", Nomos, 2020, https://dx.doi.org/10.2139/ssrn.3625712

Leonard, P., *Regulatory Trends and Emerging Practices in Access to Customer Data, Portability and Data Sharing in the Financial Services Sector* (December 3, 2017)

Lisievici, A., *Dreptul la portabilitatea datelor potrivit Regulamentului General privind Protecţia Datelor,* în I. Alexe, D.-N. Ploeşteanu, D.-M. Şandru, „Protecţia datelor cu caracter personal. Impactul protecţiei datelor personale asupra mediului de afaceri. Evaluări ale experienţelor româneşti şi noile provocări ale Regulamentului (UE) 2016/679", Editura Universitară, Bucureşti, 2017

Metzger, A., *A Market Model for Personal Data: State of Play Under the New Directive on Digital Content and Digital Services* (August 4, 2020). in Lohsse S., Schulze R., Staudenmayer D. (eds.), „Data as Counter-Performance – Contract Law 2.0?" Münster Colloquia on EU Law and the Digital Economy V, 2020

Monteleone, A. G., *Il Diritto Alla Portabilità Dei Dati. Tra Diritti Della Persona e Diritti Del Mercato*, LUISS Law Review, 2/2017

Nicholas, G., *Taking It With You: Platform Barriers to Entry and the Limits of Data Portability*, Michigan Telecommunications and Technology Law Review, 2020

Swire, P., *The Portability and Other Required Transfers Impact Assessment: Assessing Competition, Privacy, Cybersecurity, and Other Considerations*, Georgia Tech Scheller College of Business Research Paper No. 3689171, 2020, https://dx.doi.org/10.2139/ssrn.3689171

Turner, S.; Galindo Quintero, J.; Lis, J.; Tanczer, L., *The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment* (September 26, 2021), https://dx.doi.org/10.2139/ssrn.3931040

Vezzoso, S., *Competition Policy in Transition: Exploring Data Portability's Roles,* 15th ASCOLA Conference, 25-27 June 2020https://dx.doi.org/10.2139/ssrn.3634736

Vezzoso, S., *Data Portability: Initial Reflections on an Ex Ante Approach* (March 26, 2020), https://dx.doi.org/10.2139/ssrn.3561413

Vrabec, H., *Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control,* SCRIPT-ed, 2018

Vrabec, H., *The Failure of Control Rights in the Big Data Era – Does a Holistic Approach Offer a Solution?,* in Bakhoum, M., Gallego Conde, B., Mackenordt, M.-O., Surblyte, G. (eds.) „Personal Data in Competition, Consumer Protection and IP Law – Towards a Holistic Approach?", Berlin Heidelberg: Springer, 2017

Walters, R., *The Current Status of Data Portability in Personal Data and Competition Law*, European Competition Law Review, 2020

Grupul de lucru „Articolul 29" pentru protecţia datelor, „Ghid privind dreptul la portabilitatea datelor", on-line

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-5

Cunoaşterea clientelei pe piaţa criptoactivelor – între teorie şi practică

Know Your Customer on the Crypto Assets Market – Between Theory and Practice

Alina V. Popescu[1]

Rezumat: Cunoaşterea clientelei[2] reprezintă o modalitate de a evita producerea unor fraude ori implicarea în activităţi infracţionale, cum ar fi cele de spălare a banilor sau de finanţare a terorismului. Măsurile privind KYC sunt importante atât pentru mediul de afaceri, cât şi pentru clienţi şi, deşi cele mai cunoscute publicului sunt măsurile KYC pe care le aplică mediul bancar, legislaţia a extins obligativitatea aplicării acestor măsuri şi asupra altor instituţii financiare, nefinanciare şi furnizori de servicii.
Un element de noutate privind KYC îl reprezintă obligarea furnizorilor de servicii de schimb între criptoactive şi moneda fiduciară să aplice măsurile de cunoaştere a clientelei, pe fondul specificului pe care aceste active îl prezintă şi ţinând cont de faptul că aceşti furnizori îşi desfăşoară activitatea pe o piaţă nereglementată.

Cuvinte-cheie: spălarea banilor; cunoaşterea clientelei; criptoactive; pieţe nereglementate

Abstract: Knowing Your Customers is a way to avoid fraud or involvement in criminal activities, such as money laundering or terrorist financing. KYC measures are important for both business and customers, and although the best known to the public KYC measures are those applied by the banking environment, the legislation has extended the obligation to apply these measures to other financial, non-financial institutions and service providers. A novelty regarding KYC is the obligation of exchange service providers between crypto assets and fiat currency to apply measures to know the customers, on the background of the specificity of these assets and taking into account the fact that these providers operate in an unregulated market.

Keywords: money laundering; know your customer; crypto assets; unregulated market

[1] Lector univ. dr., Universitatea „Constantin Brâncoveanu” Piteşti, Facultatea de Ştiinţe Juridice, Administrative şi ale Comunicării, e-mail: avpalina_16@yahoo.com.

[2] Pe parcursul studiului vom utiliza prescurtarea KYC de la denumirea în limba engleză *„Know Your Customer”.*

1. Consideraţii generale

Deşi oferirea de servicii în domeniul criptoactivelor[3] este privită cu suspiciune de o parte a pieţei, nu se poate nega existenţa pieţei criptoactivelor şi, prin urmare, din punct de vedere juridic, problematica trebuie abordată bidimensional: pe de o parte, asigurarea unei pieţe cu risc cât mai mic pentru clienţi, pe de altă parte, prevenirea săvârşirii de infracţiuni pe o piaţă nereglementată, corelat cu conformarea furnizorilor de servicii din domeniu la prevederile legale.

Criptoactivele sunt utilizate ca depozit de valoare, precum şi ca metodă de plată pentru bunuri şi servicii legitime. Cu toate acestea, criptoactivele pot constitui mijloace de facilitare a criminalităţii, în principal pentru hackeri, elementele de crimă organizată şi teroriști.

După atacurile teroriste din anul 2001, Statele Unite ale Americii au adoptat o legislaţie referitoare la tranzacţiile financiare, prin care impuneau obligaţia de cunoaştere a clientelei ca modalitate de descurajare a finanţării terorismului.

Şi Uniunea Europeană a aliniat legislaţia din domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului, astfel încât activitatea KYC să fie cât mai bine reglementată, iar statele membre să aibă o abordare unitară, care să nu împiedice totuşi libera circulaţie a serviciilor financiare sau nefinanciare.

Raportul EU SOCTA 2021 evidenţiază faptul că: „Îmbunătăţirea legislaţiei UE în domeniul combaterii spălării banilor, având drept rezultat creşterea supravegherii financiare în sectorul bancar, a făcut să fie mai dificil, pentru reţelele criminale, să introducă venituri ilicite în economia legală prin canalele bancare tradiţionale. În consecinţă, este probabil ca încercările de spălare a banilor să fie deplasate către sectoare cu controale incipiente sau supraveghere limitată. Aceasta ar putea include utilizarea agenţiilor de remitere de bani, neautorizate, a platformelor bancare alternative[4], a comerţului internaţional şi a monedelor virtuale anonime. Utilizarea criptomonedelor este un domeniu de îngrijorare crescândă, din cauza absenţei unui regim comun de reglementare şi a nivelului de anonimat pe care îl oferă aceste produse”[5].

Totodată, raportul atenţionează că aceste criptoactive sunt din ce în ce mai utilizate pentru a efectua plăţi către oficiali corupţi, precum şi în scopuri de spălare a banilor. Acestea sunt considerate atractive pentru reţelele de infracţionalitate datorită faptului că nu sunt reglementate şi asigură o doză de anonimitate.

---

[3] Noțiunea de „criptoactive” este sinonimă, în practică, cu „criptomonede”, „active virtuale” sau „monede virtuale”. La data de 25.09.2020, a fost finalizată propunerea de Regulament al Parlamentului European și al Consiliului privind piețele criptoactivelor și de modificare a Directivei (UE) 2019/1937, [Online] la https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)593&lang=ro,accesat 30.11.2021.

[4] Situate în afara sistemului bancar tradițional, reglementat.

[5] Europol (2021), European Union serious and organised crime threat assessment, *A Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organised Crime (t.a.)*, Publications Office of the European Union, Luxembourg, [Online] la https://www.europol.europa.eu/ publication-events/main-reports/ european-union-serious-and-organised-crime-threat-assessment-socta-2021, accesat 30.11.2021.

Este important pentru instituţiile financiare, nefinanciare şi pentru furnizorii de servicii[6] să îşi cunoască clientela pentru a se putea conforma cerinţelor legale de raportare a tranzacţiilor suspecte. De aici decurge şi obligaţia de *„customer due dilligence – CDD"* a entităţilor raportoare de a solicita clienţilor mai multe informaţii, care pot include sursa fondurilor, scopul relaţiei de afaceri, ocupaţia, situaţii financiare, referinţe bancare etc., astfel încât să se atingă obiectivul KYC. Entităţile raportoare au obligaţia de a sesiza orice fel de tranzacţii suspecte şi trebuie să abordeze KYC prin prisma riscurilor pe care relaţia de afaceri le implică.

Cunoaşterea clientelei în domeniul bancar este deja o practică bine cunoscută, fapt pentru care persoanele implicate în infracţiuni de spălare a banilor şi finanţare a terorismului s-au reorientat spre alte sectoare economice, unde anonimatul este mai uşor de păstrat. O astfel de piaţă este considerată şi piaţa criptoactivelor, care se consideră că este independentă de influenţa băncilor centrale şi poate oferi variante mai facile pentru disimularea sursei fondurilor.

La fel ca în domeniul bancar, furnizorii de servicii de schimb între criptoactive şi monedă fiduciară trebuie nu doar să verifice identitatea clienţilor, ci să monitorizeze tranzacţiile derulate în platformele prin intermediul cărora furnizează serviciile, să elimine orice posibilitate de derulare a tranzacţiilor sub anonimat.

Totuşi, trebuie avut în vedere faptul că entităţile raportoare trebuie să investească sume de bani mai mari pentru a se conforma la legislaţia din materia CSB/CFT[7], ceea ce se poate traduce în costuri mai mari pentru clienţi (creşterea comisioanelor, a dobânzilor etc.). De asemenea, conformarea la legislaţia CSB/CFT poate deveni supărătoare pentru clienţi, care o consideră o birocraţie suplimentară.

Piaţa criptoactivelor, ca potenţial loc de săvârşire a unor infracţiuni, se află în atenţia autorităţilor, care trebuie să colaboreze cu furnizorii de servicii de pe această piaţă, pentru a putea atinge obiectivul de a oferi clienţilor o piaţă cât mai sigură. La nivelul Europol a fost organizată, în luna iunie 2019, o conferinţă[8] la care au participat peste 300 de experţi, atât din cadrul agenţiilor de aplicare a legii, cât şi din sectorul privat. Conferinţa a avut drept scop analizarea oportunităţilor de cooperare şi parteneriat între autorităţi şi mediul privat, pentru prevenirea şi combaterea criminalităţii legate de piaţa criptoactivelor[9]. Şi cu acest prilej, s-a reiterat importanţa implementării unor politici şi mecanisme KYC eficiente, precum şi a abordării bazate pe risc pentru tranzacţiile suspecte. De asemenea,

[6] Entități raportoare, conform prevederilor Legii nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative, publicată în Monitorul Oficial al României, Partea I, nr. 589 din 18 iulie 2019, cu modificările și completările ulterioare.

[7] Combaterea spălării banilor – CSB, combaterea finanțării terorismului – CFT.

[8] Astfel de întâlniri au fost organizate și în anii 2014-2018.

[9] Europol, Comunicat de presă, *Cryptocurrency experts meet at Europol to strengthen ties between law enforcement and private sector*, [Online] la https://www. europol. europa.eu/newsroom/news/cryptocurrency-experts-meet-europol-to-strengthen-ties-between-law-enforcement-and-private-sector, accesat 30.11.2021.

Europol a atras şi specialişti din mediul academic care să contribuie cu expertiza lor la îmbunătăţirea securităţii platformelor de tranzacţionare.

Utilizarea legitimă a criptoactivelor nu se poate realiza decât prin politici ferme în domeniul KYC, colaborarea între autorităţi şi mediul privat, asigurarea trasabilităţii tranzacţiilor realizate şi păstrarea informaţiilor despre clienţi şi tranzacţii, pentru un termen rezonabil, de regulă, stabilit de legislaţia privind CSB/CFT.

2. Prevederi legale privind obligaţia de cunoaştere a clientelei

La nivel european, Directiva (UE) 2015/849[10], în considerentul 3, invocă necesitatea unor măsuri sporite în ceea ce priveşte identificarea şi verificarea clientelei, în situaţiile cu risc mărit de spălare a banilor sau de finanţare a terorismului, precum şi de controale mai puţin riguroase, justificate de un risc mai redus, în temeiul recomandărilor din anul 2003 al Grupului de Acţiune Financiară Internaţională (FATF/GAFI)[11]. Măsurile de precauţie privind clientela includ: identificarea şi verificarea clientului şi a beneficiarului real, monitorizarea tranzacţiilor sau a relaţiei de afaceri etc.

Directiva defineşte la art. 2 care sunt entităţile obligate[12] să adopte măsurile necesare astfel încât să se prevină utilizarea sistemului financiar al Uniunii în

[10] Directiva (UE) 2015/849 a Parlamentului European şi a Consiliului din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, de modificare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului și de abrogare a Directivei 2005/60/CE a Parlamentului European și a Consiliului și a Directivei 2006/70/CE a Comisiei, publicată în Jurnalul Oficial al Uniunii Europene L 141 din 05.06.2015

[11] The Financial Action Task Force (FATF), *Who we are*, [Online] la https://www.fatf-gafi.org/about/, accesat 30.11.2021.

[12] *„Prezenta directivă se aplică următoarelor entități obligate:*

1. instituții de credit;

2. instituții financiare;

3. următoarele persoane fizice sau juridice, în exercitarea activităților lor profesionale:

(a) auditori, experți contabili externi și consilieri fiscali;

(b) notari și alte persoane care exercită profesii juridice liberale, atunci când participă, în numele și pe seama clientului, la orice tranzacție financiară sau imobiliară, sau când acordă asistență pentru planificarea sau efectuarea tranzacțiilor pentru client referitoare la:

(i) cumpărarea și vânzarea de bunuri imobile sau entități comerciale;

(ii) gestionarea banilor, a valorilor mobiliare sau a altor active ale clientului;

(iii) deschiderea sau gestionarea de conturi bancare, conturi de economii sau conturi de valori mobiliare;

(iv) organizarea contribuțiilor necesare pentru crearea, funcționarea sau administrarea societăților;

(v) crearea, funcționarea sau administrarea de fiducii, societăți, fundații sau structuri similare;

(c) furnizori de servicii pentru fiducii sau societăți care nu fac obiectul literei (a) sau (b);

(d) agenți imobiliari;

scopul spălării banilor şi finanţării terorismului. Capitolul II al Directivei (UE) 2015/849 este dedicat reglementărilor referitoare la „Precauţia privind clientela" şi stabileşte principalele măsuri ce trebuie adoptate de către entităţile obligate pentru cunoaşterea clientelei.

Prevederile Directivei (UE) 2015/849 au fost transpuse în legislaţia naţională prin adoptarea Legii nr. 129/2019[13], care preia categoriile de entităţi obligate stabilite de directivă, dar le denumeşte entităţi raportoare. De asemenea, legea defineşte noţiunea de client/clientelă, care înseamnă *„orice persoană fizică, juridică sau entitate fără personalitate juridică cu care entităţile raportoare desfăşoară relaţii de afaceri ori cu care desfăşoară alte operaţiuni cu caracter permanent sau ocazional. Se consideră client al unei entităţi raportoare orice persoană cu care, în desfăşurarea activităţilor sale, entitatea raportoare a negociat o tranzacţie, chiar dacă respectiva tranzacţie nu s-a finalizat, precum şi orice persoană care beneficiază sau a beneficiat, în trecut, de serviciile unei entităţi raportoare"*[14].

Totodată, legea stabileşte că persoanele expuse public sunt *„persoanele fizice care exercită sau au exercitat funcţii publice importante"*[15] şi determină categoriile de persoane fizice care se încadrează în noţiunea de „beneficiar real"[16].

(e) alte persoane care comercializează bunuri, numai în măsura în care plățile sunt efectuate sau încasate în numerar și au o valoare de cel puțin 10 000 EUR, indiferent dacă tranzacția se efectuează printr-o singură operațiune sau prin mai multe operațiuni care par a avea o legătură între ele;

(f) furnizorii de servicii de jocuri de noroc".

[13] Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative, publicată în Monitorul Oficial al României, Partea I, nr. 589 din 18 iulie 2019.

[14] Art. 2 lit. r) din Legea nr. 129/2019.

[15] În conformitate cu prevederile art. 3 alin. (2) din Legea nr. 129/2019, *„prin funcții publice importante se înțeleg:*

a) șefi de stat, șefi de guvern, miniștri și miniștri adjuncți sau secretari de stat;

b) membri ai Parlamentului sau ai unor organe legislative centrale similare;

c) membri ai organelor de conducere ale partidelor politice;

d) membri ai curților supreme, ai curților constituționale sau ai altor instanțe judecătorești de nivel înalt ale căror hotărâri nu pot fi atacate decât prin căi extraordinare de atac;

e) membri ai organelor de conducere din cadrul curților de conturi sau membrii organelor de conducere din cadrul consiliilor băncilor centrale;

f) ambasadori, însărcinați cu afaceri și ofițeri superiori în forțele armate;

g) membrii consiliilor de administrație și ai consiliilor de supraveghere și persoanele care dețin funcții de conducere ale regiilor autonome, ale societăților cu capital majoritar de stat și ale companiilor naționale;

h) directori, directori adjuncți și membri ai consiliului de administrație sau membrii organelor de conducere din cadrul unei organizații internaționale".

[16] Art. 4 din Legea nr. 129/2019 prevede că prin *„beneficiar real se înțelege orice persoană fizică ce deține sau controlează în cele din urmă clientul și/sau persoana fizică în numele ori în interesul căruia/căreia se realizează, direct sau indirect, o tranzacție, o operațiune sau o activitate".*

În anul 2018, a fost adoptată Directiva (UE) 2018/843[17] care observă[18] că „[f]urnizorii implicaţi în servicii de schimb între monedele virtuale şi monedele fiduciare (adică monedele şi bancnotele desemnate ca având curs legal şi moneda electronică ale unei ţări, acceptate ca mijloc de schimb în ţara emitentă), precum şi furnizorii de portofele digitale nu au nicio obligaţie stabilită de Uniune" în materie de CSB/CFT, prin urmare nu sunt constrânse să adopte măsuri în domeniul KYC, iar „anonimatul monedelor virtuale permite posibila utilizare abuzivă a acestora în scopuri criminale"[19].

Drept urmare, Directiva (UE) 2018/843 a completat art. 2 al Directivei (UE) 2015/849, incluzând în categoria entităţilor obligate „furnizorii implicaţi în servicii de schimb între monede virtuale şi monede fiduciare" şi „furnizorii de portofele digitale". Pe cale de consecinţă, aceste entităţi urmează a fi obligate de către statele membre să adopte măsuri în domeniul CSB/CFT, inclusiv măsurile în materia KYC.

România a transpus prevederile Directivei (UE) 2018/843 prin adoptarea Ordonanţei de urgenţă a Guvernului nr. 111/2020[20], astfel încât au fost incluse în categoria entităţilor raportoare furnizorii de servicii de schimb între monede virtuale şi monede fiduciare şi furnizorii de portofele digitale. Au fost definite şi noţiunile de „monede virtuale"[21] şi „furnizor de portofel"[22].

Furnizorii de servicii de schimb între monede virtuale şi monede fiduciare au fost incluşi, din punct de vedere al funcţionării, în sfera de autorizare a Ministerului Finanţelor Publice şi în sfera de supraveghere a Oficiului National de Prevenire şi

[17] Directiva (UE) 2018/843 a Parlamentului European și a Consiliului de modificare a Directivei (UE) 2015/849 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, precum și de modificare a Directivelor 2009/138/CE și 2013/36/UE, publicată în Jurnalul Oficial al Uniunii Europene L 156 din 19.06.2018.

[18] Considerentul 8 al Directivei (UE) 2018/843.

[19] Considerentul 9 al Directivei (UE) 2018/843.

[20] Ordonanța de urgență a Guvernului nr. 111/2020 privind modificarea și completarea Legii nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative, pentru completarea art. 218 din Ordonanța de urgență a Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, pentru modificarea și completarea Legii nr. 207/2015 privind Codul de procedură fiscală, precum și pentru completarea art. 12 alin. (5) din Legea nr. 237/2015 privind autorizarea și supravegherea activității de asigurare și reasigurare, publicată în Monitorul Oficial al României, Partea I, nr. 620 din 15 iulie 2020, adoptată cu modificări prin Legea nr. 101/2021, publicată în Monitorul Oficial al României, Partea I, nr. 446 din 27 aprilie 2021.

[21] Conform prevederilor art. 2 lit. t[1]) *„monede virtuale înseamnă o reprezentare digitală a valorii care nu este emisă sau garantată de o bancă centrală sau de o autoritate publică, nu este în mod obligatoriu legată de o monedă instituită legal și nu deține statutul legal de monedă sau de bani, dar este acceptată de către persoane fizice sau juridice ca mijloc de schimb și poate fi transferată, stocată și tranzacționată electronic".*

[22] Conform prevederilor art. 2 lit. t[2]) *„furnizor de portofel digital înseamnă o entitate care oferă servicii de păstrare în siguranță a unor chei criptografice private în numele clienților săi, pentru deținerea, stocarea și transferul de monedă virtuală".*

Combatere a Spălării Banilor[23], cu privire la îndeplinirea obligaţiilor de conformare la legislaţia CSB/CFT, inclusiv aceea de KYC.

Legea nr. 129/2019 stabileşte, în capitolul IV, obligativitatea entităţilor raportoare de a adopta măsuri de cunoaştere a clientelei. Măsurile standard de cunoaştere a clientelei[24] trebuie să permită:

„a) identificarea clientului şi verificarea identităţii acestuia pe baza documentelor, datelor sau informaţiilor obţinute din surse sigure şi independente, inclusiv, dacă sunt disponibile, a mijloacelor de identificare electronică şi a serviciilor de încredere relevante prevăzute de Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1.999/93/CE sau a oricărui alt proces de identificare sigur, la distanţă sau electronic, reglementat, recunoscut, aprobat sau acceptat la nivel naţional de către Autoritatea pentru Digitalizarea României;

b) identificarea beneficiarului real şi adoptarea de măsuri rezonabile pentru a verifica identitatea acestuia, astfel încât entitatea raportoare să se asigure că a identificat beneficiarul real, inclusiv în ceea ce priveşte persoanele juridice, fiduciile, societăţile, asociaţiile, fundaţiile şi entităţile fără personalitate juridică similare, precum şi pentru a înţelege structura de proprietate şi de control a clientului;

c) evaluarea privind scopul şi natura relaţiei de afaceri şi, dacă este necesar, obţinerea de informaţii suplimentare despre acestea;

d) realizarea monitorizării continue a relaţiei de afaceri, inclusiv prin examinarea tranzacţiilor încheiate pe toată durata relaţiei respective, pentru ca entitatea raportoare să se asigure că tranzacţiile realizate sunt conforme cu informaţiile deţinute referitoare la client, la profilul activităţii şi la profilul riscului, inclusiv, după caz, la sursa fondurilor, precum şi că documentele, datele sau informaţiile deţinute sunt actualizate şi relevante".

Entităţile raportoare pot să adopte şi măsuri simplificate în domeniul KYC, însă au *„responsabilitatea de a demonstra autorităţilor cu atribuţii de supraveghere şi control sau organismelor de autoreglementare că măsurile de cunoaştere a clientelei aplicate sunt corespunzătoare din punctul de vedere al riscurilor de spălare a banilor şi de finanţare a terorismului care au fost identificate"*[25].

Pe de altă parte, entităţile raportoare vor aplica măsuri suplimentare în materia KYC *„în toate situaţiile care, prin natura lor, pot prezenta un risc sporit de spălare a banilor sau de finanţare a terorismului, inclusiv în următoarele situaţii:*

a) în cazul relaţiilor de afaceri şi tranzacţiilor care implică persoane din ţări care nu aplică sau aplică insuficient standardele internaţionale în domeniul prevenirii şi combaterii spălării banilor şi a finanţării terorismului sau care sunt cunoscute la nivel internaţional ca fiind ţări necooperante;

b) în cazul relaţiilor de corespondent cu instituţii de credit şi instituţii financiare din alte state membre sau state terţe;

[23] Denumit în continuare O.N.P.C.S.B.

[24] Art. 11 alin. (1) din Legea nr. 129/2019.

[25] Art. 11 alin. (8) din Legea nr. 129/2019.

c) în cazul tranzacţiilor sau relaţiilor de afaceri cu persoanele expuse public sau cu clienţi ai căror beneficiari reali sunt persoane expuse public, inclusiv pentru o perioadă de cel puţin 12 luni începând cu data de la care respectiva persoană nu mai ocupă o funcţie publică importantă;

d) în cazul persoanelor fizice sau juridice stabilite în ţări terţe identificate de Comisia Europeană drept ţări terţe cu grad înalt de risc;

e) în cazurile prevăzute în reglementările sau instrucţiunile sectoriale emise de autorităţile competente în aplicarea prevederilor art. 1 alin. (4)"[26].

O.N.P.C.S.B. a emis Ordinul nr. 37/2021[27], incluzând furnizorii de servicii de schimb între monede virtuale şi monede fiduciare autorizaţi/înregistraţi de Ministerul Finanţelor în categoria entităţilor reglementate pentru care Oficiul este autoritatea de supraveghere şi control.

Astfel, furnizorii de servicii de schimb între monede virtuale şi monede fiduciare au obligaţia de adoptare a măsurilor KYC şi de raportare către Oficiu a tranzacţiilor suspecte, precum şi de a desemna una sau mai multe persoane cu responsabilităţi în aplicarea legislaţiei din domeniul prevenirii şi combaterii spălării banilor.

3. Aspecte practice legate de îndeplinirea obligaţiei de cunoaştere a clientelei

Conform informaţiilor Europol[28], în anul 2018, o reţea de crimă organizată a folosit criptoactive şi cărţi de credit pentru a spăla mai mult de 8 milioane de euro din traficul de droguri. Infractorii au achiziţionat criptoactive pentru a disimula sursa ilicită a veniturilor, apoi au schimbat monedele virtuale din nou în monedă fiat.

Tot în anul 2018, două reţele de crimă organizată au fost destructurate, constatându-se că au utilizat piaţa criptoactivelor pentru spălarea a 2,5 milioane de euro[29]. Membrii reţelei au achiziţionat criptomonede, pe care le-au transferat în diferite portofele digitale, pentru a disimula sursa infracţională a fondurilor.

[26] Art. 17 alin. (1) din Legea nr. 129/2019.

[27] Ordinul nr. 37 din 2 martie 2021 privind aprobarea Normelor de aplicare a prevederilor Legii nr. 129/2019 pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului, precum şi pentru modificarea şi completarea unor acte normative, pentru entităţile raportoare supravegheate şi controlate de Oficiul Naţional de Prevenire şi Combatere a Spălării Banilor, publicat în Monitorul Oficial nr. 240 din 9 martie 2021.

[28] Europol, Comunicat de presă, *Illegal network used cryptocurrencies and credit cards to launder more than EUR 8 million from drug trafficking*, [Online] la https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking, accesat 30.11.2021.

[29] Europol, Comunicat de presă, *Two criminal groups dismantled for laundering EUR 2.5 million through smurfing and cryptocurrencies*, [Online] la https://www.europol.europa.eu/newsroom/news/two-criminal-groups-dismantled-for-laundering-eur-25-million-through-smurfing-and-cryptocurrencies, accesat 30.11.2021.

În anul 2019, a fost identificat un furnizor de servicii de pe piaţa criptoactivelor[30] care s-a implicat în activităţi de spălare a banilor. Furnizorul era considerat unul dintre cei mai mari la nivel mondial (cifra de afaceri estimată pentru anul 2018 fiind de aprox. 200 milioane dolari) şi a garantat anonimatul clienţilor săi. De fapt, furnizorul oferea clienţilor un serviciu de amestecare (mixare) a criptoactivelor, astfel încât să nu mai poată fi urmărită sursa originală a criptomonedelor potenţial identificabile sau „contaminate". Ancheta a reliefat faptul că multe dintre criptomonedele mixte de pe site-ul furnizorului de servicii aveau o origine sau o destinaţie infracţională, serviciile furnizorului fiind utilizate pentru a ascunde şi spăla fluxuri infracţionale de bani.

În luna februarie 2021, a fost destructurată o grupare de criminalitate organizată[31] care utiliza, pentru disimularea originii ilicite a veniturilor, *dark web*[32] şi platforme de tranzacţionare a criptoactivelor.

Aplicarea măsurilor KYC de către entităţile obligate trebuie să se facă ţinând cont de un echilibru, astfel încât procedurile să nu devină greoaie pentru clienţi sau costisitoare pentru entitate ori să afecteze libera concurenţă din domeniile reglementate. Procesul de cunoaştere a clientelei include pe de o parte programul de identificare a clienţilor (*Customer Identification Program* – CIP) şi, pe de cealaltă parte, manifestarea unei diligenţe corespunzătoare în relaţia cu clienţii (*Customer Due Diligence* – CDD).

În practică, apar diferite situaţii cu care se confruntă furnizorii de servicii de schimb între monede fiduciare şi criptoactive, cum ar fi refuzul clienţilor de a furniza datele cu caracter personal, sursa ori cuantumul veniturilor. Din acest motiv, la înregistrarea pe o platformă de tranzacţionare a criptoactivelor, identificarea clienţilor trebuie să se facă ţinând cont de asigurarea protecţiei datelor furnizate, să utilizeze tehnologii noi, avansate, capabile să facă o recunoaştere corectă şi să asigure conexiunea cu alte baze date date. Tehnologia trebuie să fie flexibilă, uşor de folosit, prietenoasă cu utilizatorul (de exemplu, serviciile să fie oferite cu interfaţa în mai multe limbi). Totodată, utilizarea unor servicii de identificare automată este în măsură să asigure conformarea la legislaţia CSB/CFT.

Furnizorii de servicii de verificare automată a identităţii oferă beneficiarilor (instituţii financiare, furnizori de servicii de schimb între monede fiduciare şi

[30] Europol, Comunicat de presă, *Multi-million euro cryptocurrency laundering service Bestmixer.io taken down*, [Online] la https://www.europol.europa.eu/ newsroom/news/ multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down, accesat 30.11.2021.

[31] Europol, Comunicat de presă, *International drug trafficking network disrupted,* [Online] la https://www.europol.europa.eu/newsroom/news/international-drug-trafficking-network-disrupted, accesat 30.11.2021.

[32] *„Termenul dark web se referă la conținut online criptat care nu este indexat de motoarele de căutare convenționale. Accesarea web-ului întunecat se poate face numai folosind anumite browsere, cum ar fi TOR Browser. Utilizarea dark web în comparație cu site-urile web tradiționale asigură o mai mare confidențialitate și anonimat"* [tr.n], [Online] la https://www.investopedia.com/terms/d/dark-web.asp, accesat 30.11.2021.

criptoactive etc.) posibilitatea de cunoaşte clientela prin verificarea identităţii lor în bazele de date privind persoanele expuse politic (aşa-numitele *„PEP lists”*), în listele globale privind sancţiunile internaţionale (*global sanctions lists*), în bazele de date guvernamentale ori ale organizaţiilor internaţionale privind persoanele urmărite (*watchlist*), precum şi prin identificarea ştirilor negative apărute despre persoanele respective (*adverse media & negative news*).

Tot în cadrul proceselor KYC şi CDD, furnizorii de servicii de schimb între monede fiduciare şi criptoactive pot crea liste de supraveghere a clientelei (*internal watchlists*) care să includă clienţi deja înrolaţi în aplicaţie, dar care prezintă suspiciuni sau clienţi cu care s-a încheiat relaţia de afaceri din motive de suspiciune de fraudă ori CSB/CFT. Verificarea potenţialilor clienţi în aceste liste interne previne reînrolarea unui client cu grad de risc ridicat.

Aşa cum arătam în secţiunea introductivă, abordarea pe bază de riscuri a procesului KYC poate conduce la necesitatea solicitării de informaţii suplimentare de la client, atunci când riscul este pe cale să crească (spre exemplu, volumul sau frecvenţa tranzacţiilor creşte) şi entitatea raportoare trebuie să manifeste prudenţă privind derularea relaţiei comerciale, pentru reducerea riscurilor putând lua chiar decizia de a întrerupe derularea relaţiei de afaceri.

În ceea ce priveşte persoanele expuse public, în practică, trebuie avut în vedere că simpla apartenenţă a unei persoane la categoria respectivă nu trebuie să împiedice derularea unei relaţii comerciale, întrucât nu se poate pleca de la premisa că aceste persoane au săvârşit o ilegalitate. Cunoaşterea trebuie făcută la fel ca în cazul celorlalţi clienţi şi, doar dacă există suspiciuni privind tranzacţiile sau sursa fondurilor, să se aplice măsuri suplimentare de cunoaştere a acestora.

În ceea ce priveşte tranzacţiile suspecte, în practică, la analizarea operaţiunilor de schimb între criptoactive şi moneda fiduciară, trebuie să se aibă în vedere: complexitatea tranzacţiilor, valori neobişnuit de mari tranzacţionate, comportamentul uzual al clientului, scopul tranzacţiei, pentru a preîntâmpina realizarea unei tranzacţii cu risc ridicat.

4. Concluzii

Furnizarea de servicii de schimb între criptoactive şi monedă fiduciară este o activitate exclusiv digitală. Într-o eră a digitalizării, în care fraudele informatice cunosc de asemenea o creştere semnificativă, investiţiile realizate pentru a face o bună cunoaştere a clientelei, deşi pot părea costisitoare, sunt importante atât pentru siguranţa afacerii, cât şi pentru menţinerea unei reputaţii neştirbite.

Dacă se va dovedi că piaţa criptoactivelor se extinde, furnizorii de servicii de pe această piaţă trebuie să adopte măsuri care să uşureze înrolarea pe platformă (de exemplu, utilizarea unor formulare cu autocompletare sau cu răspunsuri predefinite din care clientul poate alege, utilizarea serviciilor de identificare automată ş.a.), concomitent cu conformarea la cerinţele legale în materie.

În situaţia în care furnizorii de servicii de schimb între criptoactive şi monedă fiduciară nu respectă obligaţiile legale în domeniul KYC, aceasta poate atrage, după caz, răspunderea civilă, disciplinară, contravenţională, administrativă sau penală.

O.N.P.C.S.B. este abilitat să constate contravenţiile şi să aplice sancţiunile, cu menţiunea că, prin derogare de la prevederile O.G. nr. 2/2001[33], aplicarea sancţiunii amenzii contravenţionale se prescrie în termen de 5 ani de la data săvârşirii faptei.

De asemenea, pentru o prevenţie eficientă a fenomenului infracţional de spălare a banilor, este importantă cooperarea autorităţilor, a agenţiilor de aplicare a legii şi furnizorii de servicii de pe piaţa criptoactivelor.

Referinţe

Europol (2021), European Union serious and organised crime threat assessment, A Corrupting Influence: *The Infiltration and Undermining of Europe's Economy and Society by Organised Crime (t.a.)*, Publications Office of the European Union, Luxembourg

Europol, Comunicat de presă, *Cryptocurrency experts meet at Europol to strengthen ties between law enforcement and private sector*

Europol, Comunicat de presă, *Illegal network used cryptocurrencies and credit cards to launder more than EUR 8 million from drug trafficking*

Europol, Comunicat de presă, *Two criminal groups dismantled for laundering EUR 2.5 million through smurfing and cryptocurrencies*

Europol, Comunicat de presă, *Multi-million euro cryptocurrency laundering service Bestmixer.io taken down*

Europol, Comunicat de presă, *International drug trafficking network disrupted*

[33] Ordonanţa Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare, publicată în Monitorul Oficial al României, Partea I, nr. 410 din 25 iulie 2001.

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-6

Aspecte teoretice şi jurisprudenţiale privind respectarea GDPR la încheierea şi executarea unui contract

Theoretical and Jurisprudential Aspects Regarding GDPR Compliance When Concluding or Performing a Contract

Mirela-Carmen Dobrilă[1]

Rezumat: Dreptul la protecţia datelor cu caracter personal reprezintă un drept fundamental care trebuie protejat la nivel european şi la nivel global, iar Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016, Regulamentul general privind protecţia datelor (RGPD/GDPR), a reformat cadrul destinat să asigure protecţia datelor cu caracter personal, asigurând repere clare şi certitudine cu privire la prelucrarea datelor cu caracter personal ale persoanelor în condiţii de siguranţă. În articol sunt analizate condiţiile care trebuie respectate, conform RGPD/ GDPR pentru prelucrarea datelor cu caracter personal atunci când temeiul legal al prelucrării este articolul 6 alin. (1) litera b din RGPD/ GDPR, adică atunci când prelucrarea datelelor cu caracter personal este necesară pentru a executa un contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract, cu unele corelaţii şi cu alte temeiuri legale pentru prelucrare; în articol sunt indicate şi unele repere din jurisprudenţa europeană relevantă în acest sens.

Cuvinte-cheie: date cu caracter personal; respectarea RGPD/GDPR; Regulamentul (UE) 2016/679; încheierea sau executarea unui contract; temei legal pentru prelucrarea datelor

Abstract: The right to the protection of personal data is a fundamental right that must be protected at European and global level, and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, General Regulation on Data Protection (RGPD / GDPR), reformed the framework regarding the protection of personal data, ensuring clear conditions of processing and certainty for the processing of personal data of persons in safe conditions. The article analyzes the conditions to be met, according to the RGPD / GDPR for the processing of personal data when the legal basis for the processing is Article 6 (1) (b) of the RGPD / GDPR, ie when the processing of personal data is necessary to perform a contract to which the data subject is a party or to take action at the request of the data subject before concluding a contract, with some correlations and other legal grounds for processing; the article also highlights some relevant European case law.

Keywords: personal data; GDPR compliance; Regulation (EU) 2016/679; concluding or executing a contract; legal basis for data processing

[1] Lector univ. dr., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iaşi, email: mirela.dobrila@uaic.ro.

1. Consideraţii generale privind prelucrarea datelor cu caracter personal în temeiul Regulamentului (UE) 2016/679. Temeiuri legale de prelucrare

Regulamentul (UE) 2016/679[2] (RGPD[3]/GDPR[4]) reprezintă cadrul unic şi coerent de reglementare la nivelul Uniunii Europene privind protecţia datelor cu caracter personal ale persoanei fizice/persoanei vizate, cu scopul de a asigura protecţia vieţii private a persoanelor fizice şi, în acelaşi timp, scopul de a asigura libera circulaţie a datelor cu caracter personal, în contextul unei pieţe unice la nivel european. Regulamentul a reformat la nivel european cadrul destinat să asigure protecţia datelor cu caracter personal, în conformitate cu principiile (indicate în art. 5 RGPD) privind: legalitatea, echitatea şi transparenţa în prelucrarea datelor cu caracter personal; limitările legate de scopurile prelucrării care trebuie să fie determinat, explicite şi legitime; reducerea doar la ceea ce este necesar cu privire la datele prelucrate; prelucrarea unor date exacte şi actualizate; limitările legate de stocare, adică o prelucrare a datelor cu caracter personal pentru perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; necesitatea de a asigura o securitate adecvată a datelor cu caracter personal, adică asigurarea măsurilor de securitate şi confidenţialitate.

Regulamentul (UE) 2016/679 are aplicabilitate generală şi se aplică direct în toate ţările membre ale Uniunii Europene; acesta a fost semnat la 27 aprilie 2016, este în vigoare la data de 25 mai 2016, dar se aplică din data de 25 mai 2018[5]. Regulamentul (UE) 2016/679 vizează protecţia persoanelor fizice la un vinel ridicat şi în mod consecvent, iar protecţia să fie asigurată în mod echivalent la nivelul tuturor statelor membre[6].

Protecţia datelor cu caracter personal reprezintă dreptul fundamental din art. 8 din Carta drepturilor fundamentale a Uniunii Europene[7]. Conform art. 39 din Tratatul privind Uniunea Europeană (TUE) şi art. 16 din Tratatul privind funcţionarea Uniunii Europene (TFUE), orice persoană are dreptul la protecţia datelor cu caracter personal care o privesc, iar prelucrarea datelor cu caracter personal ale persoanei fizicese poate realiza doar pe baza unui temei legal indicat de

[2] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din data de 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), JO L 119, 4.5.2016.

[3] Acronimul RGPD vizează *Regulamentul General privind Protecţia Datelor.*

[4] Acronimul GDPR vizează *General Data Protection Regulation.*

[5] A se vedea și Rectificarea la Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), JO L 119, 4.5.2016.

[6] A se vedea considerentul 10 din Regulamentul (UE) 2016/679.

[7] Carta drepturilor fundamentale a Uniunii Europene, JO C 326, 26.10.2012.

Regulamentul (UE) 2016/679 (art. 6, resspectiv art. 9 pentru datele cu caracter special).

Conform art. 71 din Codul civil[8], orice persoană are dreptul la respectarea vieţii sale private, fiind interzisă utilizarea, în orice mod, a corespondenţei, manuscriselor sau a altor documente personale, precum şi a informaţiilor din viaţa privată a unei persoane, fără acordul acesteia ori fără respectarea limitelor stabilite de lege[9].

Conform art. 2 RGPD, regulamentul este aplicabil pentru prelucrarea datelor cu caracter personal, realizată prin mijloace automatizate (total sau parţial) sau nu, care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un astfel de sistem. Conform art. 3 RGPD, regulamentul vizează prelucrarea datelor cu caracter personal în cadrul activităţilor unui sediu al unui operator/persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii, dar se aplică şi cu privire la prelucrarea datelor cu caracter personal ale persoanelor vizate care se află în Uniune de către un operator (sau persoană împuternicită de acesta) care nu este stabilit în Uniune, dacă prelucrarea este legată de oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăţi de către persoana vizată, sau monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

Atunci când temeiul legal al prelucrării este articolul 6 alin. (1) litera b din RGPD, adică atunci când prelucrarea datelelor cu caracter personal este necesară pentru a executa unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract, este necesar să analizăm care sunt datele cu caracter personal care pot fi prelucrate pe

[8] *Noul Cod civil*, Legea nr. 287/2009, republicată, M. Of. 505 din 15 iulie 2011.

[9] Conform art. 74 din Codul civil, pot fi considerate ca atingeri aduse vieţii private: *„a) intrarea sau rămânerea fără drept în locuinţă sau luarea din aceasta a oricărui obiect fără acordul celui care o ocupă în mod legal; b) interceptarea fără drept a unei convorbiri private, săvârşită prin orice mijloace tehnice, sau utilizarea, în cunoştinţă de cauză, a unei asemenea interceptări; c) captarea ori utilizarea imaginii sau a vocii unei persoane aflate într-un spaţiu privat, fără acordul acesteia; d) difuzarea de imagini care prezintă interioare ale unui spaţiu privat, fără acordul celui care îl ocupă în mod legal; e) ţinerea vieţii private sub observaţie, prin orice mijloace, în afară de cazurile prevăzute expres de lege; f) difuzarea de ştiri, dezbateri, anchete sau de reportaje scrise ori audiovizuale privind viaţa intimă, personală sau de familie, fără acordul persoanei în cauză; g) difuzarea de materiale conţinând imagini privind o persoană aflată la tratament în unităţile de asistenţă medicală, precum şi a datelor cu caracter personal privind starea de sănătate, problemele de diagnostic, prognostic, tratament, circumstanţe în legătură cu boala şi cu alte diverse fapte, inclusiv rezultatul autopsiei, fără acordul persoanei în cauză, iar în cazul în care aceasta este decedată, fără acordul familiei sau al persoanelor îndreptăţite; h) utilizarea, cu rea-credinţă, a numelui, imaginii, vocii sau asemănării cu o altă persoană; i) difuzarea sau utilizarea corespondenţei, manuscriselor ori a altor documente personale, inclusiv a datelor privind domiciliul, reşedinţa, precum şi numerele de telefon ale unei persoane sau ale membrilor familiei sale, fără acordul persoanei căreia acestea îi aparţin sau care, după caz, are dreptul de a dispune de ele”.*

baza acestui temei legal de prelucrare şi care depăşesc sfera acestuia, fiind făcute delimitări faţă de prelucrarea pe baza altor temeiuri legale (de exemplu consimţământul persoanei vizate).

2. Protecţia datelor cu caracter personal la încheierea şi executarea unui contract – art. 6 alin. (1) lit. b)RGPD

Conform art. 4 pct. 1 din RGPD, *datele cu caracter personal* sunt orice informaţii privind o persoană fizică identificată sau identificabilă (numită persoana vizată), iar *persoană fizică identificabilă* înseamnă[10] „o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale". Operatorul este definit ca persoana fizică sau juridică, autoritatea, agenţia, alt organism, care stabileşte „scopurile şi mijloacele prelucrării" (art. 4 alin. (1) pct. 7 RGPD), iar scopul prelucrării se stabileşte pe baza temeiului juridic (art. 4 alin. 3 teza finala RGPD).

Prelucrarea datelor cu caracter legal este legală dacă se realizează în condiţiile art. 6 din RGPD (respectiv pentru datele cu caracter special, în condiţiile art. 9 RGPD[11]), adică pe baza unui temei juridic indicat: (a) persoana vizată şi-a dat

[10] Unele aspecte privind semnificaţia unor noţiuni au fost analizate anterior în M. C. Dobrilă, *Particularităţi privind noţiunea de date cu caracter personal necesare pentru încheierea sau executarea unui contract la care persoana vizată este parte*, Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" Iaşi, Tomul LXVII, Supliment, Ştiinţe Juridice, 2021, pp. 211-225, [Online] la http://pub.law.uaic.ro/ files/articole/2021/vol.2_ 1/15.dobrila.pdf, accesat 10.11.2021, şi în M. C. Dobrilă, *RGPD/GDPR: prelucrarea datelor cu caracter personal la încheierea/executarea unui contract. Unele particularităţi privind prelucrarea datelor cu caracter personal în condiţiile crizei COVID-19*, Volumul Sesiunii anuale de comunicări ştiinţifice a Institutului de Cercetări Juridice „Acad. Andrei Rădulescu" al Academiei Române – „Starea excepţională şi alerta ordinii de drept. Implicaţii juridice ale crizei sanitare generată de pandemia Covid-19", 2021, pp. 77-86; spre deosebire de UE, în SUA există mai multe definiţii pentru datele cu caracter personal, fiind folosită sintagma „personally identifiable information", fără a se distinge între persoana identificată şi persoana identificabilă. A se vedea C.T. Ungureanu, *Protecţia datelor cu caracter personal în contractele internaţionale*, în Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" Iaşi, Tomul LXIII, Ştiinţe juridice, nr. 2/2017, p. 4, [Online] la http://pub.law.uaic.ro/files/articole/2017/volii/10.ungureanu_protectia_datelor.pdf, accesat 20.11.2021.

[11] Conform art. 9 alin. (2) RGPD, prelucrarea datelor personale cu caracter special poate fi realizată doar dacă: *„(a) persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepţia cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicţia prevăzută la alineatul (1) să nu poată fi ridicată prin consimţământul persoanei vizate; (b) prelucrarea este necesară în scopul îndeplinirii obligaţiilor şi al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forţei de muncă şi al securităţii sociale şi protecţiei sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanţii*

consimţământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice; (b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract; (c) prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului; (d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice; (e) prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul; (f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terţă, cu excepţia cazului

adecvate pentru drepturile fundamentale și interesele persoanei vizate; (c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul; (d) prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filosofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate; (e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată; (f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare; (g) prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate; (h) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alineatul (3); (i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional; sau (j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate". Datele personale cu caracter special sunt definite de art. 9 alin. (1) RGPD ca *„date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la sindicate şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viaţa sexuală sau orientarea sexuală ale unei persoane fizice".*

în care prevalează interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil".

Referitor la temeiul juridic din articolul 6 alin. (1) litera b din RGPD, privind prelucrarea datelor cu caracter personal „necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract", trebuie avute în vedere două aspecte:

- o prelucrare a datelor cu caracter personal necesare pentru executarea unui contract la care persoana vizată este parte;

- o prelucrare a datelor cu caracter personal atunci când este necesară pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract.

În cazul în care prelucrarea datelor cu caracter personal se bazează pe temeiul interesului legitim sau pe executarea unui contract, nu este permisă o colectare şi o prelucrare a datelor în mod excesiv în raport cu scopul specificat[12].

Referitor la etapele încheierii şi executării unui contract, sunt avute în vedere în mod distinct momentul anterior încheierii contractului, adică etapa negocierilor şi a încheierii contractuui, respectiv un moment ulterior încheierii contractului, adică etapa executării contractului.

Referitor la prima ipoteză, *prelucrarea datelor cu caracter personal necesară pentru încheierea unui contract,* temeiul juridic privind această ipoteză vizează demersurile la cererea persoanei vizate iar, sub aspect temporal, aceste să aibă loc înainte de încheierea unui contract.

Temeiul juridic privind încheierea contractului priveşte relaţiile precontractuale, cu condiţia să se ia măsuri la cererea persoanei vizate, „mai degrabă decât la iniţiativa operatorului sau a oricărui terţ", cum ar fi de exemplu cazul persoanei fizice care solicită unui asigurător informaţii privind prima de asigurare în vederea sigurării unui autovehicul iar asigurătorul este îndreptăţit să prelucreze date privind maşina, model, vechime pentru a reliza o ofertă[13] (persoana fiind identificată sau identificabilă); sau, de exemplu, această ipoteză priveşte comunicarea datelor cu caracter personal de către persoana vizată către comerciant în vederea comunicării de către un comerciant a unei oferte pentru un bun, fiind necesare informaţii privind adresa, informaţii cu privire la ceea ce s-a solicitat, colectarea fiind realizată pentru operiadă limitată de timp.

Dacă însă ar fi solicitate date privind antecedentele medicale pentru o asigurare de sănătate sau o asigurare de viaţă, sau verificarea informaţiilor privind creditele anterior acordării unui împrumut, acestea nu sunt considerate măsuri

[12] Pentru dezvoltări a se vedea Grupul de lucru „Articolul 29" (GL29) , *Avizul 06/2014 privind noțiunea de interese legitime ale operatorului de date în temeiul articolului 7 din Directiva 95/46/CE (WP 217),* adoptat la 9 aprilie 2014, p. 12 [Online] la https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_ro.pdf, accesat 20.11.2021.

[13] *Idem*, p. 19.

necesare efectuate la cererea persoanei vizate, ci prelucrarea se poate realiza pe baza unui alt temei juridic[14], de exemplu, interesul legitim.

Cu toate acestea, verificarea antecedentelor, de exemplu, prelucrarea datelor legate de vizitele medicale înainte ca o societate de asigurări să ofere unui solicitant o asigurare de sănătate sau o asigurare de viaţă, nu ar fi considerate măsuri necesare efectuate la cererea persoanei vizate. De asemenea, controalele informaţiilor privind creditele înainte de acordarea unui împrumut nu sunt efectuate *la cererea* persoanei vizate, în conformitate cu articolul 7 litera (b), ci mai degrabă în conformitate cu articolul 7 litera (f) sau în conformitate cu articolul 7 litera (c) în temeiul unei obligaţii legale a băncilor de a consulta o listă oficială a debitorilor înregistraţi.

Pentru a doua situaţie, temeiul juridic vizează *prelucrarea necesară pentru executarea unui contract la care persoana vizată este parte,* iar interpretarea trebuie făcută în mod strict.

Temeiul juridic privind „prelucrarea necesară pentru executarea unui contract" nu acoperă situaţiile în care prelucrarea nu este cu adevărat necesară pentru executarea unui contract, deoarece trebuie ca prelucrarea să fie necesară pentru a executa contractul pentru fiecare persoană vizată în parte (prelucrarea numelui, adresei sau a datelor privind cardul persoanei vizate pentru executarea unui contract de vânzare încheiat online cu privire la executarea obligaţiei de predare, respectiv de plată; prelucrarea informaţiilor referitoare la salarii şi a detaliilor privind conturile bancare pentru salariaţi în cadrul unui contract de muncă)[15].

Cu titlu de exemplu, temeiul juridic privind prelucrarea necesară pentru executarea unui contract la care persoana vizată este parte poate include prelucrarea adresei persoanei fizice pentru livrarea bunurilor cumpărate online sau prelucrarea datelor privind cardurile de credit pentru a efectua plata, cu privire la raporturile de muncă, temeiul poate permite prelucrarea informaţiilor privind salariile şi conturile bancare pentru a se efectua plata[16].

Pentru a avedea dacă poate fi aplicat temeiul juridic privind prelucrarea necesară pentru executarea unui contract", trebuie să corelată evaluarea necesităţii şi respectarea principiului limitării scopului, fiind necesar să fie clar stabilite motivele încheierii contractului şi conţinutul său, în funcţie de care se verifică dacă prelucrarea datelor este necesară pentru executarea acestuia (de exemplu stabilirea unei baze de date cu informaţiile de contact ale angajaţilor, , adică numele, adresa comercială, numărul de telefon şi adresele de email ale angajaţilor, pentru a permite angajaţilor să intre în contact cu colegii lor, poate fi considerată necesară, în anumite situaţii, pentru executarea unui contract; supravegherea video, monitorizarea

[14] *Idem*, p. 20.

[15] GL29, *op. cit.*, p. 18; European Data Protection Board (Comitetul european pentru protecţia datelor- EDPB), *Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679*, 4 mai 2020, p. 11, [Online] la https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_ro.pdf, accesat 21.08.2021.

[16] GL29, *op. cit.*, p. 18.

electronică a utilizării internetului, a emailului sau a telefonului de către angajaţi este o prelucrare care este probabil să depăşească ceea ce este necesar pentru executarea unui contract de muncă, dar depinde de natura locului de muncă sau prelucrarea poate fi legitimă dacă a fost acordat consimţământul în acest sens)[17].

Temeiul juridic indicat la art. 6 alin. (1) lit. b)RGPD se aplică dacă prelucrarea nu depăşeasşte ceea ce este necesar pentru executarea normală a unui contract.

Dacă prelucrarea datelor cu caracter personal vizează încheierea sau executarea unui contract, nu înseamnă întotdeauna că prelucrarea este esenţială în acest scop, însă aceasta trebuie să fie limitată la şi proporţională cu scopul urmărit[18].

Nu se poate aplica pentru toate prelucrările de date în legătură cu un contract temeiul indicat la art. 6 alin. (1) lit. b)RGPD, pentru simplul fapt că sunt în legătură cu un contract

De exemplu, se consideră că monitorizarea şi crearea de profiluri depăşesc ceea ce este necesar pentru executarea unui contract deoarece scopul pentru care a fost contactat operatorul de către persoana vizată se referă la cumpărarea de bunuri şi servicii şi nu la crearea de profiluri, nefiind necesare pentru executarea contractului.

Nu trebuie făcută confuzie între temeiul juridic privind consimţământul persoanei vizate şi temeiul juridic privind prelucrarea necesară pentru încheierea sau executarea unui contract; nici nu se poate invoca temeiul juridic privind consimţământul exprimat pentru prelucrarea datelor cu caracter personal care de fapt sunt necesare pentru încheierea unui contract sau executarea unui contract la care persoana vizată este parte deoarece temeiul juridic va fi cel din art. 6 alin.1 lit. b)RGPD.

În acest sens există situaţii în care consimţământul este inclus în contracte sau prestarea unui serviciu este condiţionată de acordarea consimţământului[19], deşi trebuie făcută o corectă apreciere a temeiului juridic; pentru prelucrarea datelor cu caracter personal necesare pentru încheierea sau executarea contractului, în condiţiile prevăzute de art. 6 alin.1 lit. b)RGPD, acesta va fi temeiul juridic, iar pentru prelucrarea altor date cu caracter personal, care nu sunt necesare pentru încheierea sau executarea contractului, temeiul juridic va putea fi consimţământul.

Referitor la prelucrarea datelor cu caracter personal pe temeiul art. 6 alin. (1), lit. a)(consimţământul persoanei vizate), este necesar să fie îndeplinite anumite condiţii pentru a fi valabil consimţământul exprimat: să fie explicit şi specific, să fie informat, lipsit de ambiguitate, să fie separat, să fie revocabil (cu posibilitatea de a fi retras la fel de uşor cum a fost dat).

În plus, furnizarea unui serviciu solicitat de / oferit persoanei vizate nu poate fi condiţionată de acordarea consimţământului pentru prelucrare din partea

[17] GL29, *op. cit.*, p. 18.

[18] Uniunea Națională a Barourilor din România (UNBR), *Ghid de bune practici privind principalele obligații ale avocaților conform Regulamentului General privind Protecția Datelor* (GDPR), 4 aprilie 2018, p. 16, [Online] la https://www.unbr.ro/wp-content/uploads/2018/04/DATE-PERSONALE-Ghid-de-Bune-Practici_v04042018.pdf, accesat 25.11.2021.

[19] EDPB, *op. cit.*, p. 8.

respectivei persoane deoarece consimţământul nu ar fi liber exprimat. În acest sens, conform art. 7 alin. (4) RGPD, „când se evaluează dacă consimţământul este dat în mod liber, se ţine seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiţionată sau nu de consimţământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract".

Este important să existe posibilitatea executării contractului sau a furnizării serviciului de către operatorul respectiv fără acordarea consimţământului pentru prelucrarea de date suplimentare, ceea ce înseamnă că serviciul nu mai este condiţionat[20]. Cele două temeiuri juridice, consimţământul şi contractul, nu pot fi unite şi nu se pot confunda.

Referitor la obligaţiile avocaţilor şi la temeiul juridic privind prelucrarea necesară pentru încheierea şi executarea unui contract, în Ghidul UNBR pentru avocaţi privind GDPR se inidică faptuş că prelucrarea datelor părţii adverse nu se poate întemeia pe contractul de asistenţă juridică încheiat cu clientul (poate fi un alt temei, de exemplu interesul public)[21]. Iar abordarea de către avocat a unui client nou, persoană fizică, fără o manifestare de interes din partea primului nu poate avea ca temei viitorul contract de asistenţă juridică[22].

Prelucrarea pe baza temeiului juridic privind executarea unui contract sau pentru încheierea unui contract este considerată legală doar dacă există un contract valabil încheiat conform reglementărilor din dreptul contractelor.

Curtea de Justiţie a Uniunii Europene s-a pronunţat în Hotărârea Breyer, din 19 octombrie 2016, în sensul că articolul 7 litera f) din Directiva 95/46/CE se opune „unei dispoziţii de drept naţional în temeiul căreia un furnizor de servicii de comunicaţii electronice poate colecta şi utiliza datele cu caracter personal aferente unui utilizator în lipsa consimţământului acestuia numai în măsura în care această colectare şi această utilizare sunt necesare pentru a permite şi a factura utilizarea concretă a serviciilor respective de către acest utilizator şi în temeiul căreia finalitatea care constă în asigurarea funcţionalităţii generale a aceloraşi servicii nu poate justifica utilizarea datelor după o sesiune de consultare a acestora"; se arată că „prelucrarea datelor cu caracter personal în sensul acestei dispoziţii este legală în cazul în care este necesară în scopul realizării interesului legitim urmărit de operator sau de terţul ori de terţii cărora le sunt comunicate datele, cu condiţia să nu prevaleze interesul sau drepturile şi libertăţile fundamentale ale persoanei vizate. Or, în speţă, legislaţia germană a exclus în mod categoric şi generalizat posibilitatea ca anumite categorii de date cu caracter personal să fie prelucrate, fără a permite o ponderare a drepturilor şi a intereselor opuse în cauză într-un anumit caz"[23].

[20] EDPB, *op. cit.*, p. 13.

[21] UNBR, *op. cit.,* p. 15.

[22] *Ibidem.*

[23] Curtea de Justiție a Uniunii Europene, *Hotărârea din 19 octombrie 2016 Patrick Breyer împotriva Bundesrepublik Deutschland. (C-582/14),* [Online] la https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX%3A62014CJ0582, accesat 01.11.2021; Curtea de

Referitor la temeiul juridic pentru prelucrarea datelor, există un interes crescut cu privire la utilizarea dispozitivelor de supraveghere video, cu justificări care ţin, de exemplu, de securitate, însă acestea trebuie utilizate prudent şi cu respectarea drepturilor persoanei vizate (de exemplu montarea unui sistem de supraveghere video de către proprietarul unui magazin pentru a preveni furtul, vandalismul, deci pe baza temeiului juridic privind interesul legitim[24], conform art. 6 alin. (1) lit. f RGPD ; sau pentru monitorizarea antrenamentelor sportivilor, pe temeiul juridic privind consimţământul - art. 6 alin. (1) lit. a)RGPD[25]). Pentru prelucrarea datelor rezultate din monitorizarea prin sisteme video se poate utiliza temeiul juridic privind încheierea sau executarea uni contract, art. 6 alin. (1) lit. b) RGPD. Se consideră în orientările de la nivel european că oricare dintre temeiurile juridice prevăzute la articolul 6 alin. (1) poate constitui temei juridic pentru prelucrarea datelor provenite din supravegherea video, deşi cele mai utilizate sunt interesul legitim şi necesitatea de a îndeplini o sarcină care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice, iar în mod excepţional, consimţământul[26].

Cu privire la temeiul legal privind încheierea sau executarea unui contract, recent, a fost formulată o cerere adresată Curţii de Justiţie a Uniunii Europene pentru a răspunde la următoarele întrebări preliminare[27]: „Atunci când un utilizator de internet fie doar consultă site-uri sau aplicaţi care au legătură cu criteriile prevăzute la articolul 9 alineatul (1) din RGPD[28], cum ar fi aplicaţii de flirt, site-uri de întâlniri pentru homosexuali, site-uri ale partidelor politice, site-uri de sănătate, fie introduce date pe aceste site-uri, cum ar fi cu ocazia înregistrării sau a

---

Justiție a Uniunii Europene, Direcția de Cercetare și Documentare, *Fișă tematică- Protecția datelor cu caracter personal,* iulie 2020, p. 21, p. 11, [Online] la https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_ro.pdf, accesat 01.11.2021; În Cauza Breyer C-582/14 s-a reținut și faptul că „adresă de protocol internet dinamică înregistrată de un furnizor de servicii de comunicații electronice cu ocazia consultării de către o persoană a unui site internet pe care acest furnizor îl pune la dispoziția publicului constituie, pentru furnizorul respectiv, o dată cu caracter personal în sensul acestei dispoziții, în cazul în care acesta dispune de mijloace legale care îi permit să identifice persoana vizată cu ajutorul informațiilor suplimentare de care dispune furnizorul de acces la internet al acestei persoane".

[24] European Data Protection Board (Comitetul european pentru protecţia datelor/ CEPD), Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video, versiunea 2.0, doptat la 29 ianuarie 2020, p. 11, [Online] la https://edpb. europa.eu/ sites/ default/files/files/file1/ edpb_guidelines_201903_video_devices_ro.pdf, accesat 11.11.2021.

[25] *Idem,* p. 15.

[26] *Idem,* p. 10.

[27] Cerere de decizie preliminară introdusă de Oberlandesgericht Düsseldorf (Germania) la 22 aprilie 2021 – Facebook Inc. și alții/Bundeskartellamt (Cauza C-252/21), [Online] la https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:62021CN0252&from=RO, accesat 12.11.2021.

[28] N.n.: articolul 9 alineatul (1) din RGPD se referă la prelucrarea de date cu caracter special.

comenzilor, iar o altă întreprindere precum Facebook Ireland colectează date referitoare la consultarea site-urilor şi a aplicaţilor de către utilizator şi pe cele introduse de acesta pe site-urile respective, prin intermediul interfeţelor integrate în site-uri şi în aplicaţii, precum 'Instrumentele Facebook pentru afaceri' sau prin intermediul modulelor cookie instalate pe computerul sau pe echipamentul terminal mobil al utilizatorului de internet ori al unor tehnologii de stocare similare, asociază aceste date cu datele contului Facebook.com al utilizatorului şi le utilizează în privinţa colectării şi/sau a asocierii şi/sau a utilizării, este vorba despre prelucrarea a unor date sensibile în sensul acestei dispoziţii?" ; în cazul unui răspuns afirmativ (în sensul considerării acestor date ca date sensibile), s-a solicitat o clarificare cu privire la următorul aspect: dacă „consultarea acestor site-uri şi aplicaţii şi/sau introducerea unor date şi/sau acţionarea butoanelor integrate în aceste site-uri sau aplicaţii ('pluginuri sociale' precum 'Îmi place', 'Distribuie' sau 'Conectare Facebook' ori 'Account Kit') ale unui furnizor precum Facebook Ireland echivalează cu a face publice în mod manifest datele referitoare la consultare ca atare şi/sau la datele introduse de utilizator în sensul articolului 9 alineatul (2) litera (e) din RGPD?", precum şi cu privire la temeiul legal pentru prelucrare, fie temeiul privind executarea contractului, fie interesul legitim: „O întreprindere precum Facebook Ireland care exploatează o reţea socială digitală, finanţată din publicitate, care, în condiţiile sale de utilizare, pune la dispoziţie personalizarea conţinuturilor şi a publicităţii, securitatea reţelei, îmbunătăţirea produselor şi utilizarea coerentă şi uniformă a tuturor produselor grupului, poate invoca justificarea întemeiată pe necesitatea executării contractului în conformitate cu articolul 6 alineatul (1) litera (b) din RGPD sau pe realizarea unor interese legitime în conformitate cu articolul 6 alineatul (1) litera (f) din RGPD atunci când, în aceste scopuri, întreprinderea respectivă colectează date din alte servicii ale grupului şi de pe site-uri şi aplicaţii terţe prin intermediul interfeţelor integrate în acestea precum „Instrumentele Facebook pentru afaceri" sau al modulelor cookie instalate pe computerul sau pe echipamentul terminal mobil al utilizatorului de internet ori al unor tehnologii de stocare similare, le asociază cu contul Facebook.com al utilizatorului şi le utilizează?".

Referitor la situaţia în care a fost aplicată o amendă amendă unei societăţi înregistrate în Slovacia care administrează pagini de internet de anunţuri imobiliare privind bunuri situate în Ungaria, pentru motivul că aceasta nu a procedat la eliminarea datelor cu caracter personal ale autorilor anunţurilor acestor situri, în pofida cererii lor în acest sens, şi a comunicat aceste date către agenţii de recuperare a creanţelor pentru a obţine achitarea unor facturi neplătite, Curtea de Justiţie a Uniunii Europene s-a pronunţat în Hotărârea Weltimmo din 1 octombrie 2015 (C-230/14) în sensul că „articolul 4 alineatul (1) litera (a) din Directiva 95/46/CE permite aplicarea legislaţiei privind protecţia datelor cu caracter personal a unui alt stat membru decât statul în care operatorul responsabil cu prelucrarea acestor date este înregistrat, în măsura în care acesta exercită, într-o formă de instalare stabilă pe teritoriul acestui stat membru, o activitate efectivă şi reală, fie şi minimă, în cadrul căreia este efectuată prelucrarea. Pentru a determina dacă

aceste condiţii sunt îndeplinite, instanţa de trimitere poate îndeosebi să ţină cont de faptul, pe de o parte, că activitatea operatorului de date în cadrul căreia are loc prelucrarea constă în exploatarea unor site-uri internet de anunţuri imobiliare”[29].

În anumite situaţii, în funcţie de natura, domeniul de aplicare, contextul şi scopurile prelucrării, în cazul în care prelucrarea (mai ales atunci când este vorba de utilizarea noilor tehnologii) este susceptibilă să genereze un risc ridicat pentru drepturile persoanei fizice, operatorul va trebui să efectueze o evaluare a impactului operaţiunilor de prelucrare, anterior prelucrării datelor. De observat faptul că prin excepţie[30], atunci când prelucrarea datelor se realizează pe temeiul juridic privind încheierea sau executarea contractului, art. 6 alin. (1) lit. b)RGPD, evaluarea impactului asupra protecţiei datelor nu este obligatorie.

În condiţiile evoluţiei accelerate a tehnologiei digitale şi a intensificării comerţului electronic, asistăm la o creştere a riscurilor de utilizare online a datelor referitoare la cărţile de credit, cu efecte negative faţă de persoana vizate deoarece datele financiare pot fi utilizate pentru fraudarea sistemelor de plată.

În acest sens, referitor la problema privind stocarea de către furnizorii online de bunuri şi servicii, în scopul unic şi specific de a facilita achiziţiile ulterioare ale persoanelor vizate, există recomenări la nivel european cu privire la stocarea datelor referitoare la cărţile de credit de către furnizorii online de bunuri şi servicii, cu scopul de a asigura o facilitare a achiziţiilor ulterioare realizat de persoana vizată. Referitor la persoana vizată care „cumpără un produs sau plăteşte un serviciu prin intermediul unui site sau al unei aplicaţii şi furnizează datele referitoare la cartea sa de credit, în general într-un formular special, pentru a încheia respectiva tranzacţie unică”, mai întâi avem în vedere faptul că operatorul trebuie să aibă un temei juridic valabil conform art. 6 RGPD pentru stocarea datelor respective.

Se consideră că stocarea datelor referitoare la cărţile de credit după efectuarea plăţii pentru bunuri sau servicii „nu este necesară ca atare pentru executarea unui contract [articolul 6 alineatul (1) litera (b) din RGPD]” şi chiar dacă prelucrarea datelor privind cartea de credit utilizată de client pentru a plăti este necesară în primul rând pentru executarea contractului (art. 6 alin. (1) lit. b)RGPD), „stocarea acestor date este utilă numai pentru a facilita o potenţială tranzacţie viitoare şi pentru a facilita vânzările”, însă „un astfel de scop nu poate fi considerat

[29] Curtea de Justiție a Uniunii Europene, *Hotărârea din 1 octombrie 2015, Weltimmo s.r.o. împotriva Nemzeti Adatvédelmi és Információszabadság Hatóság*, [Online] la https://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1446203751915&uri=CELEX:62014CJ0230, accesat 01.11.2021; CJUE, *Fișă tematică- Protecția datelor cu caracter personal*, *op. cit.*, p. 46.

[30] A se vedea art. 1 alin. (2) din Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 174 din 18 octombrie 2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal, [Online] la https://www.dataprotection.ro/servlet/View Document?id=1556, accesat 3.11. 2021.

strict necesar pentru executarea contractului de furnizare a bunului sau a serviciului pe care persoana vizată l-a plătit deja”[31].

În ceea ce priveşte furnizarea de servicii online persoanelor vizate, operatorii sunt obligaţi să verifice respectarea principiilor privind protecţia datelor cu caracter personal şi a tuturor cerinţelor RGPD, precum şi a legislaţiei privind confidenţialitatea în mediul electronic[32]. Din perspectiva legalităţii, contractele pentru servicii online trebuie să fie valabile în temeiul legislaţiei aplicabile în domeniul contractelor[33].

3. Consideraţii finale privind prelucrarea datelor cu caracter personal pe baza temeiului legal din art. 6 alin. (1) lit b RGPD

Prelucrarea datelor cu caracter personal este legală dacă se realizează în condiţiile art. 6 RGPD, respectiv pentru prelucrarea datelor sensibile, în condiţiile art. 9 RGPD. Conform art. 6 alin. (1) lit. b)RGPD, prelucrarea datelor cu caracter personal se realizează pe baza temeiului legal privind prelucrarea „necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract”, fiind avute în vedere două ipoteze: prelucrarea este necesară pentru a face demersuri, în special, la cererea persoanei vizate şi situaţia în care prelucrarea „necesară pentru executarea unui contract la care persoana vizată este parte. Atunci când temeiul juridic vizează încheierea sau executarea contractului nu trebuie făcută confuzie cu temeiul juridic privind consimţământul persoanei vizat- art. 6 alin. (1) lit. a)RGPD e, care trebuie să fie liber şi iar executarea contractului sau prestarea unui serviciu nu pot fi condiţionate de acordarea consimţământului pentru date suplimentare faţă de cele necesare pentru încheierea sau executarea contractului, iar cele două temeiuri juridice – contract, consimţământ, nu pot fi unite şi nici nu trebuie confundate; nu orice prelucrare de date cu caracter personal în legătură cu un contract îndeplineşte condiţiile cu privire la aplicarea temeiului juridic privind contractul- art. 6 alin. (1) lit. b)RGPD.

Referinţe

***Cerere de decizie preliminară introdusă de Oberlandesgericht Düsseldorf (Germania) la 22 aprilie 2021 – Facebook Inc. şi alţii/Bundeskartellamt (Cauza C-252/21)

[31] Comitetul European pentru Protecţia Datelor, *Recomandările nr. 02/2021 privind temeiul juridic pentru stocarea datelor referitoare la cărțile de credit în scopul unic de a facilita alte tranzacții online,* adoptate la 19 mai 2021, p. 3, [Online] la https://edpb.europa.eu/system/files/2021-07/recommendations022021_on_storage_of_credit_card_data_ro.pdf, accesat 12.11.2021.

[32] A se vedea Comitetul European pentru Protecţia Datelor, *Orientările 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate*, versiunea 2.0, 8 octombrie 2019, pp. 5-6, [Online] la https://edpb.europa.eu/sites/ default/files/files/file1/ edpb_ guidelines-art_ 6-1-b-adopted_after_public_consultation_ro.pdf,accesat 21.11.2021.

[33] *Idem*, p. 6.

Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, Decizia nr. 174 din 18 octombrie 2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal

Comitetul European pentru Protecţia Datelor, *Orientările 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate*, versiunea 2.0, 8 octombrie 2019

Comitetul European pentru Protecţia Datelor, *Recomandările nr. 02/2021 privind temeiul juridic pentru stocarea datelor referitoare la cărţile de credit în scopul unic de a facilita alte tranzacţii online*, adoptate la 19 mai 2021

Curtea de Justiţie a Uniunii Europene, Direcţia de Cercetare şi Documentare, *Fişă tematică- Protecţia datelor cu caracter personal*, iulie 2020

Curtea de Justiţie a Uniunii Europene, *Hotărârea din 1 octombrie 2015, Weltimmo s.r.o. împotriva Nemzeti Adatvédelmi és Információszabadság Hatóság*

Curtea de Justiţie a Uniunii Europene, *Hotărârea din 19 octombrie 2016 Patrick Breyer împotriva Bundesrepublik Deutschland. (C-582/14)*

Dobrilă M.-C., *RGPD/GDPR: prelucrarea datelor cu caracter personal la încheierea/executarea unui contract. Unele particularităţi privind prelucrarea datelor cu caracter personal în condiţiile crizei COVID-19*, Volumul Sesiunii anuale de comunicări ştiinţifice a Institutului de Cercetări Juridice „Acad. Andrei Rădulescu" al Academiei Române – „Starea excepţională şi alerta ordinii de drept. Implicaţii juridice ale crizei sanitare generată de pandemia Covid-19", 2021, pp. 77-86

Dobrilă, M.-C., *Particularităţi privind noţiunea de date cu caracter personal necesare pentru încheierea sau executarea unui contract la care persoana vizată este parte*, Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" Iaşi, Tomul LXVII, Supliment, Ştiinţe Juridice, 2021, pp. 211-225, DOI: https://doi.org/10.47743/jss-2021-67-3-15

European Data Protection Board (Comitetul european pentru protecţia datelor), Orientările 05/2020 privind consimţământul în temeiul Regulamentului 2016/679, 4 mai 2020

Grupul de lucru „Articolul 29", *Avizul 06/2014 privind noţiunea de interese legitime ale operatorului de date în temeiul articolului 7 din Directiva 95/46/CE (WP 217)*

Ungureanu, C.T., *Protecţia datelor cu caracter personal în contractele internaţionale*, în Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" Iaşi, Tomul LXIII, Ştiinţe juridice, nr. 2/2017

Uniunea Naţională a Barourilor din România, *Ghid de bune practici privind principalele obligaţii ale avocaţilor conform Regulamentului General privind Protecţia Datelor (GDPR)*, 4 aprilie 2018

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-7

Aspecte legale privind licitaţiile de artă online

Legal Aspects Regarding On-line Art Auctioning

Vlad Vieriu[1]

Rezumat: *Lato sensu,* patrimoniul cultural mobil se suprapune peste o arie mult mai extinsă a vieţii noastre culturale, mult peste dimensiunea strict tehnică a bunurilor clasate în patrimoniul cultural mobil naţional. Civilizaţia umană contemporană este astăzi interesată de viaţa sa culturală mai mult decât niciodată. Circulaţia bunurilor culturale s-a intensificat odată cu creşterea apetitului pentru cultură, pe fondul unei perioade postbelice de pace şi prosperitate. Mijloacele tehnice au permis treptat gestionarea drepturilor asupra bunurilor culturale la distanţă, iar apogeul a fost atins în momentul în care încheierea la distanţă a actelor juridice a devenit o necesitate în timpul pandemiei. Astfel a luat naştere un univers aparte al licitaţiilor de artă online, ale cărui particularităţi juridice sunt de actualitate.

Cuvinte-cheie: patrimoniu cultural mobil; licitaţie online; artă; contracte încheiate la distanţă

Abstract: Lato sensu, the moveable cultural heritage overlaps a much wider area of our cultural life, much more than the strictly technical dimension of objects which are listed in the national moveable cultural heritage. The contemporary human civilization is interested, now more than ever, in its cultural life. The circulation of cultural property has intensified with the increase in the interest in culture, in the light of a peaceful and prosper post war period. The technical means have allowed the remote management of rights on cultural property, and its peek was reached when the conclusion of legal acts turned into a necessity during the pandemic. Thus, a specific universe of on-line art auctioning came to light, and its legal particularities are of current interest.

Keywords: moveable cultural heritage; on-line auctioning; art; remote legal acts

Creativitatea fiinţei umane nu cunoaşte limite, fiind dintotdeauna o inepuizabilă resursă de civilizaţie, frumos şi fericire. Creaţiile omului, purtătoare de identitate, se disting prin trăsăturile şi valoarea lor, deopotrivă muabile. În mod natural sau accidental, materiale sau imateriale, creaţiile suferă eroziuni şi metamorfoze dintre cele mai variate şi nu toate au şansa de a supravieţui împotriva timpului, a factorilor naturali sau a acţiunilor umane. Cele ce se impun în conştiinţa culturală a omului o fac în virtutea valorii pe care o au, valoare dependentă de criteriile şi moravurile ce conturează această conştiinţă. Marile monumente ale

[1] Doctor în drept, cadru didactic asociat, Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iași, e-mail: vlad.vieriu@uaic.ro.

Antichităţii greco-latine, *exempli gratia*, au fost create ca mari opere ale culturii şi civilizaţiei epocii, pentru a fi mai apoi abandonate, îngropate, desconsiderate, pentru a fi din nou redescoperite cu titlu de inestimabile elemente ale patrimoniului cultural al omenirii, în Epoca Modernă şi Epoca Contemporană. Treptat, au apărut şi s-au impus în ultimele secole o ştiinţă, o disciplină şi un drept al patrimoniului cultural pentru a asigura mediul optim în care interesele culturale generale să se realizeze prin cele mai restrânse, dar mai eficiente atingeri aduse drepturilor particularilor asupra bunurilor culturale, iar una dintre prerogativele cele mai importante a fost dintotdeauna cea a circulaţiei juridice a bunurilor culturale. Dinamica bunurilor culturale este cu atât mai accentuată astăzi, în condiţiile în care formele de expresie artistică s-au diversificat în siajul evoluţiei tehnologice din ultimele decenii. Cert este că arta şi bunurile de patrimoniu sunt preţuite şi căutate, fiind o investiţie cu prea puţine riscuri care să planeze asupra valorii acestora, iar pe fondul acestei realităţi economice şi culturale incontestabile s-a dezvoltat în timp o fascinantă piaţă a bunurilor culturale.

Istoria licitaţiilor publice este veche, fiind atestată de menţiuni precum cele ale istoricului grec Herodot sau cele privind procedura *manus injectio* pe care o regăsim în dreptul roman. În civilizaţia romană sunt întâlnite şi primele licitaţii ale unor bunuri cu vocaţie cultural-artistică, în cadrul procedurilor de executare silită împotriva debitorilor – *venditio bonorum* şi *distractio bonorum*[2]. Răspândirea accentuată a creştinismului oficializat, începând cu domnia împăratului Constantin cel Mare a însoţit civilizaţia europeană spre Evul Mediu, în care viaţa culturală a Europei a cunoscut o altă intensitate, considerabil diminuată faţă de ceea ce fusese şi ceea ce avea să fie. Pe fondul Renaşterii, licitaţiile culturale au reapărut în Europa în Secolul al XVII-lea, prin iniţiativa particulară a unor pasionaţi din clasele medii ale Ţărilor de Jos sau Italiei, apoi prin mijlocirea unor anunţuri în publicaţii din marile capitale europene, pentru ca în 1674 să-şi deschidă porţile prima casă de licitaţii din Europa – Stockholms Auktionsverk[3]. În secolul următor au urmat vinderea la licitaţie a impresionantei colecţii aparţinând contelui Eduard de Oxford şi apariţia caselor de licitaţii Sothesby's în anul 1744 şi Christie's în anul 1766. Piaţa bunurilor culturale a continuat să se dezvolte semnificativ de-a lungul Secolului al XIX-lea, alimentată de colonialism şi bunăstare, până la începutul marii crize din prima jumătate a Secolului al XX-lea, într-o primă fază, apoi până la cel de-al Doilea Război Mondial. A doua conflagraţie mondială a ruinat întreaga Europă şi viaţa culturală a acesteia, iar circulaţia bunurilor culturale a avut nevoie de timp pentru a se reface, dar realizările tehnologice şi economice din deceniile postbelice, precum comunicaţiile prin telefon şi satelit, au avut o contribuţie semnificativă la revigorarea licitaţiilor culturale. Interesul pentru artă a sporit constant şi odată cu acesta şi preţurile de adjudecare, iar bunurile culturale şi-au descoperit vocaţia de a fi o investiţie sigură. Piaţa de artă nu a regresat, ba dimpotrivă, a cunoscut ultimul

[2] V.M. Ciucă, *Drept roman. Lecțiuni,* ed. a II-a, Editura Universității „Alexandru Ioan Cuza", Iaşi, 2014, p. 147.

[3] Artland, *Going Once, Going Twice, Sold! A Short History of Art Auctions,* [Online] la https://magazine.artland.com/a-short-history-of-art-auctions/, accesat 4.12.2021.

apogeu simbolic în anul 2017, atunci când opera *Salvator Mundi* a lui Leonardo da Vinci a fost adjudecată pentru nu mai puţin de 450.300.000 USD[4].

Actualmente, piaţa bunurilor culturale cunoaşte două ipostaze. Pe de o parte avem parte de o efervescentă piaţă primară, ce priveşte bunurile culturale noi, ce fac obiectul vânzării pentru prima dată de la momentul creării lor. Pe de altă parte, o altă statură, mai impunătoare, cunoaşte piaţa secundară, cea a bunurilor culturale ce fac obiectul unor înstrăinări subsecvente, vizibilă îndeosebi cu ocazia evenimentelor organizate special pentru a vinde şi a dobândi creaţiile – licitaţiile de artă. Dincolo de dimensiunea lor pur juridică, acestea s-au impus de-a lungul ultimelor secole ca fenomene în sine a căror solemnitate priveşte prea puţin sfera condiţiilor de validitate a actelor juridice ce se încheie cu această ocazie. Orientarea caselor de licitaţii şi a persoanelor interesate spre dimensiunea online s-a realizat în mod firesc şi aşteptat, mijloacele şi tehnicile informatice fiind prezente nu doar la nivelul asigurării posibilităţii de a participa la licitaţii de la distanţă, ci şi la cel al monedelor virtuale de plată sau chiar în esenţa creaţiilor, *exempli gratia* a NFT-urilor. Apărute încă dinainte de izbucnirea pandemiei cu noul coronavirus SARS CoV 2 în anul 2020, alternativele online au fost treptat adoptate pentru a surmonta distanţele şi a diminua riscurile epidemiologice.

Fără a avea anvergura marilor pieţe de artă occidentale, cea autohtonă rămâne totuşi remarcabilă, în condiţiile în care aceasta este naturalmente dependentă de cuantumul resurselor pe care le „exploatează", iar fondul cultural al României este la rându-i dependent de stadiul evoluţiei societăţii româneşti sub aspect istoric, cultural, demografic, educaţional etc. Cea mai importantă casă de licitaţii a bunurilor culturale din România este Artmark, care îşi desfăşoară activitatea din anul 2008, având un portofoliu impresionant din care nu lipsesc aproape toţi marii artişti plastici ai României. Începând cu anul 2019 Artmark a pus la dispoziţia persoanelor interesate platforma Artmak LIVE®, pentru a permite participarea la licitaţii de la distanţă, online. Artmark va fi modelul de referinţă la care vom apela pentru a ilustra legităţile proprii licitaţiilor bunurilor culturale în România, prin prisma normelor juridice incidente.

Obiectul succintei noastre analize priveşte exclusiv licitaţiile publice organizate în scopul vinderii şi al cumpărării bunurilor culturale alienabile în virtutea libertăţii contractuale şi a autonomiei de voinţă, în contextul evenimentelor culturale organizate *ad-hoc,* şi nu priveşte situaţiile particulare de executare silită a bunurilor mobile ce ar putea fi întâlnite în cazul în care bunurile ce fac obiectul urmăririi silite mobiliare ar face parte din patrimoniul cultural naţional sau ar avea relevanţă cultural-artistică. De altfel, în lumina prevederilor art. 727 lit. e) C. proc. civ., *scrisorile, fotografiile şi tablourile personale sau de familie şi altele asemenea nu sunt supuse urmăririi silite,* ceea ce le oferă însă şansa de a fi înstrăinate la licitaţiile culturale.

O menţiune necesară în acest context o reprezintă faptul că, în privinţa licitaţiilor publice privind obiectele de artă şi alte bunuri culturale, nu sunt

[4] *Ibidem.*

aplicabile prevederile Legii nr. 449 din 12 noiembrie 2003[5] Republicată[6] privind vânzarea produselor şi garanţiile asociate acestora. Astfel, potrivit art. 3 din lege, *„nu sunt supuse prevederilor prezentei legi produsele folosite care sunt vândute prin procedura licitaţiei publice, la care consumatorul are posibilitatea să participe personal”.* Această excepţie reprezintă expresia transpunerii în legislaţia României a prevederilor art. 1 par. (3) din Directiva 1999/44/CE a Parlamentului European şi a Consiliului din 25 mai 1999 privind anumite aspecte ale vânzării de bunuri de consum şi garanţiile conexe[7]. În altă ordine de idei, cumpărătorul ce participă la licitaţia publică de bunuri culturale nu se situează sub aria de acoperire a imperativului de protecţie a consumatorului, motiv pentru care sunt ineficiente în acest domeniu şi prevederile O.G. nr. 21 din 21 august 1992[8] Republicată[9] privind protecţia consumatorilor.

Deşi cunoscute în limbajul comun cu titlul de „licitaţii de artă”, *stricto sensu,* licitaţia rămâne doar punctul culminant al unor veritabile ritualuri de societate cu semnificative implicaţii juridice, care încep în momentul cristalizării ofertelor mutuale şi se desăvârşesc prin predarea bunului cumpărat la licitaţie persoanei care a fost declarată câştigătoare. Atât din perspectivă teoretică, dar şi din punct de vedere practic, raporturile care se nasc şi momentele pe care le parcurge transmiterea dreptului de proprietate asupra unui bun cultural de la o persoană la alta se coagulează în două etape structurale, casa de licitaţii fiind elementul de legătură, persoana împuternicită a media încheierea actului translativ de proprietate. Vehiculul juridic utilizat pentru a conduce dreptul de proprietate din patrimoniul înstrăinătorului în cel al dobânditorului este în acest caz contractul de consignaţie. Readus în albia dreptului civil după suprimarea dreptului comercial ca ramură de sine stătătoare, varietate a contractului de comision, care la rându-i reprezintă o specie a mandatului fără reprezentare, contractul de consignaţie *„are ca obiect vânzarea unor bunuri mobile pe care consignantul le-a predat consignatarului în acest scop”,* potrivit prevederilor art. 2.054 C. civ. Definiţia legală a contractului de consignaţie stipulează în mod expres caracteristica unui contract real, predarea bunurilor mobile fiind o condiţie de valabilitate a contractului. Revenind la cele două etape despre care am făcut vorbire anterior, literatura

[5] Monitorul Oficial al României, Partea I, nr. 347 din 6 mai 2008.

[6] Republicată în temeiul prevederilor art. V lit. n) din titlul III din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianţilor în relaţia cu consumatorii şi armonizarea reglementărilor cu legislaţia europeană privind protecţia consumatorilor, publicată în Monitorul Oficial al României, Partea I, nr. 899 din 28 decembrie 2007, dându-se textelor o nouă numerotare.

[7] Directiva 1999/44/CE a Parlamentului European şi a Consiliului din 25 mai 1999 privind anumite aspecte ale vânzării de bunuri de consum şi garanţiile conexe, *publicată în Jurnalul Oficial al Uniunii Europene L 171, 7.7.1999, p. 12–16.*

[8] Monitorul Oficial al României, Partea I, nr. 208 din 28 martie 2007.

[9] Republicată în temeiul art. V din Legea nr. 476/2006 pentru modificarea şi completarea Ordonanţei Guvernului nr. 21/1992 privind protecţia consumatorilor, publicată în Monitorul Oficial al României, Partea I, nr. 1.018 din 21 decembrie 2006, dându-se textelor o nouă numerotare.

juridică civilistă a observat şi a atras atenţia asupra faptului că se impune a fi făcută distincţia dintre efectele contractului ce se produc între consignant şi consignatar, pe de o parte, şi cele ce se produc ca urmare a executării de către consignatar a obligaţiei specifice, respectiv cele izvorând din contractul de vânzare încheiat de consignatar cu terţa parte[10], o distincţie ce se evidenţiază în mod deosebit în contextul încheierii şi executării contractului de consignaţie având ca obiect bunuri mobile culturale.

În privinţa obiectului derivat al licitaţiilor culturale, acesta este reprezentat de o sferă foarte cuprinzătoare de bunuri exclusiv mobile având o inerentă valoare artistică, arhivistică, numismatică, ştiinţifică, literară etc. Nu fac obiectul analizei noastre bunurile imobile relevante din punct de vedere cultural, pentru simplul motiv că înstrăinarea acestora urmează un traseu aparte, nefiind exclusă *de plano* nici în ipoteza acestora vânzarea în urma unei licitaţii publice. Tablouri, icoane, grafică, hărţi de colecţie, cărţi, manuscrise, documente de arhivă, fotografii, afişe, piese de numismatică, sculpturi, artă sacră, obiecte industriale de patrimoniu, artă contemporană, artă decorativă, bijuterii, ceasuri, obiecte de artizanat, piese de mobilier, covoare, piese de vestimentaţie, instrumente muzicale, viniluri şi casete audio, arme şi armuri, autoturisme de epocă, aparate de zbor, vinuri şi alte băuturi alcoolice, toate acestea şi nu numai alcătuiesc esenţa materială a circulaţiei bunurilor culturale universale.

Rafinat în peste un deceniu de existenţă, modelul Artmarkt este, în opinia noastră, un autentic sistem de referinţă pentru spaţiul românesc, atât din perspectivă social-culturală, cât şi din perspectivă juridică, o confirmare a eficienţei şi optimizării unor soluţii teoretice şi practice care să armonizeze interesele persoanelor ce participă la licitaţiile de artă, indiferent de calitatea acestora, pe de o parte, şi interesele generale ale statului şi societăţii cu privire la patrimoniul cultural naţional, privit deopotrivă în dimensiune statică şi dinamică, pe de altă parte. Cadrul contractual general conceput de casa de licitaţii Artmark este configurat în cele mai importante linii ale sale de două regulamente proprii ce conferă substanţă fiecărui contract de consignaţie privit *ut singuli: Regulament consignare*[11], respectiv, *Regulament de licitare*[12]. Circuitul consignaţiei este iniţiat prin depunerea operelor la sediul consignatarului. Identitatea deponentului este protejată de o clauză de confidenţialitate, cu excepţia cazului în care acesta optează pentru dezvăluirea identităţii sale. Pasul imediat următor îl reprezintă expertizarea şi evaluarea operei, cu titlu gratuit în cazul casei de licitaţii Artmark, un pas determinant atât pentru însăşi formarea contractului de consignaţie şi susţinerea cauzei pentru încheierea actului, în ceea ce-l priveşte pe consignant, cât şi pentru

[10] F.-A. Baias, E. Chelaru, R. Constantinovici, I. Macovei (coord.), *Noul Cod civil. Comentariu pe articole*, ed. a II-a. revizuită și adăugită, Editura C.H. Beck, București, 2014, p. 2198.

[11] Artmark, *Regulament consignare,* [Online] la https://www.artmark.ro/ro/reguli-de-consignare, accesat 5.12.2021.

[12] Artmark, *Regulament de licitare,* [Online] la https://www.artmark.ro/ro/reguli-licitatie, accesat 5.12.2021.

interesele inerente activităţii specifice a consignatarului. Valoarea de piaţă a operei este stabilită de o entitate proprie consignatarului – Biroul de Evaluare şi Custodie – prin determinarea unei limite valorice minime şi a unui interval valoric estimativ funcţional, care să asigure vânzarea bunului într-o perspectivă realistă. În continuare, proprietarul operei păstrează opţiunea de a încheia sau nu contractul de consignaţie. Pentru casa de licitaţii, cauza proximă a contractului o reprezintă comisionul de vânzare ce urmează a fi reţinut în urma vânzării operei la licitaţie, comision a cărui valoare variază în funcţie de numărul şi valoarea operelor, precum şi de performanţa operei în licitaţie. Limita valorică maximă a intervalului prezintă interes în situaţia aplicării unor sancţiuni contractuale consignantului, precum în cazul în care acesta retrage opera din consignaţie înainte de expirarea termenului agreat de părţi, sau în cazul în care o terţă persoană contestă dreptul deponentului de a vinde la licitaţie opera, iar consignatarul, în urma unei analize proprii, apreciază că există îndoieli substanţiale cu privire la dreptul deponentului de a vinde opera. De altfel, consignantul garantează autenticitatea operei şi dreptul său de proprietate asupra operei, exonerându-l pe consignatar de orice formă de răspundere faţă de terţii adjudecatari şi urmând a suporta orice prejudiciu adus deopotrivă acestora şi consignatarului însuşi. Încheierea unui contract de consignaţie cu casa de licitaţii Artmak atrage şi asumarea unei clauze de conexitate şi interdependenţă a rezultatelor licitaţiei curente în raport de eventualele obligaţii născute în urma unor raporturi anterioare. De asemenea, cheltuielile ce excedează cadrul specific al vinderii prin licitaţie în cadrul casei, precum cele de curăţare, restaurare, depozit prelungit sau expediţie pentru restituire, vor fi suportate de consignant. În urma reţinerii vor fi virate şi eventualele sarcini fiscale datorate pentru cazul în care consignantul este şi autorul operei. Pentru a conchide în spiritul elaborării analizei noastre orientate spre dimensiunea online a licitaţiilor de artă, putem afirma faptul că, cel puţin până la momentul perfectării contractului de consignaţie, spaţiul virtual rămâne închis, iar contractul de consignaţie îşi manifestă deplin caracterul real. Concluzia aceasta este, din punctul nostru de vedere, foarte importantă pentru că evidenţiază caracterul special al vânzării bunurilor culturale şi al regimului juridic al acesteia, punându-l într-o lumină diferită faţă de omniprezentul shopping online atât de dezvoltat în ultimii ani.

A doua etapă este reprezentată de licitaţia de obiecte de artă care, cu titlu de regulă, se desfăşoară la sediul casei de licitaţii sau într-un alt loc stabilit în prealabil de aceasta. Având în vedere că obiectele se vând în starea în care acestea se află, eventualii cumpărători ce au intenţia de a participa la licitaţie au posibilitatea de a le inspecta, inclusiv de a apela la concursul unui specialist în acest scop. Pentru a facilita observarea de la distanţă a obiectelor ce urmează a fi vândute, casa de licitaţie pune la dispoziţie online un raport de condiţie cu privire la starea de conservare a obiectului. Aceste măsuri vin în întâmpinarea eventualelor nemulţumiri şi vicii care ar putea fi invocate ulterior adjudecării. În altă ordine de idei, pentru adjudecatarii care se limitează exclusiv la o participare online la licitaţie, nu vor putea refuza plata, ci vor fi deplin obligaţi. Participarea de la distanţă la licitaţiile casei Artmark este posibilă fie prin intermediul unui cont

online pe platforma Artmark LIVE®, în prezenţă sau în absenţă, cu ajutorul unei *„palete electronice de licitaţie”,* fie telefonic, fie prin plasarea unei oferte scrise online, prin completarea unui formular. În cazul unor oferte multiple aparţinând unor participanţi în absenţă se aplică principiul *qui prior temporis, potior jure,* însă ordinea generală de prioritate conferă întotdeauna întâietate ofertelor venind din sala de licitaţie. Participarea proprietarilor bunurilor culturale sau a interpuşilor acestora contravine convenţiei părţilor în mod imperativ. În urma licitaţiei consumate, adjudecatarul va fi ţinut să plătească preţul de adjudecare la care se adaugă taxa totală de licitaţie ce include TVA şi orice alte taxe asociate dobândirii operei pe teritoriul României, potrivit legislaţiei în vigoare. În cazul casei de licitaţii Artmark, taxa totală de licitaţie este de 20% din preţul de adjudecare. Denunţarea unilaterală a vânzării la licitaţie nu este posibilă. Finalmente, vânzarea încheiată astfel este executată prin plata preţului, în urma emiterii facturii şi predarea bunului adjudecat.

Dincolo de trunchiul comun al normelor de drept privat ce constituie domeniul de reglementare principal în privinţa circulaţiei bunurilor culturale, fie aceasta înlesnită de mijloacele proprii mediului online, se impune a evidenţia coexistenţa şi specificul unor norme speciale de ordin administrativ care au scopul de a asigura o gestionare optimă a patrimoniului cultural naţional, norme pe care le regăsim fie în H.G. nr. 1.420 din 4 decembrie 2003 pentru aprobarea Normelor privind comerţul cu bunuri culturale mobile[13], fie în Legea nr. 182 din 25 octombrie 2000[14] Republicată[15] privind protejarea patrimoniului cultural naţional mobil. De asemenea, de o deosebită importanţă pentru a determina limitele intrinseci ale comerţului legitim având ca obiect bunuri culturale sunt prevederile O.G. nr. 43 din 30 ianuarie 2000[16] Republicată[17] privind protecţia patrimoniului arheologic şi declararea unor situri arheologice ca zone de interes naţional. În pofida lacunelor inerente procesului tehnico-legislativ, actul normativ anterior amintit trasează o linie certă de demarcaţie între bunurile care pot face obiectul aproprierii şi circulaţiei juridice între particulari şi bunurile care nu fac parte din circuitul civil, datorită importanţei culturale deosebite a acestora. Demarcaţia aceasta se suprapune în concret peste frontiera dintre comerţul şi exportul legitim al bunurilor culturale şi piaţa clandestină, ilegală, care profită substanţial de avantajele pe care le oferă mediul online.

[13] Monitorul Oficial al României, Partea I, nr. 900 din 16 decembrie 2003.

[14] Monitorul Oficial al României, Partea I, nr. 530 din 27 octombrie 2000.

[15] Republicată în temeiul art. 248 din Legea nr. 187/2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal, publicată în Monitorul Oficial al României, Partea I, nr. 757 din 12 noiembrie 2012, rectificată în Monitorul Oficial al României, Partea I, nr. 117 din 1 martie 2013, cu modificările ulterioare, dându-se textelor o nouă numerotare.

[16] Monitorul Oficial al României, Partea I, nr. 900 din 16 decembrie 2003.

[17] Republicată în temeiul art. IV din Legea nr. 258/2006 pentru modificarea şi completarea Ordonanţei Guvernului nr. 43/2000 privind protecţia patrimoniului arheologic şi declararea unor situri arheologice ca zone de interes naţional, publicată în Monitorul Oficial al României, Partea I, nr. 603 din 12 iulie 2006, dându-se textelor o nouă numerotare.

Cu titlu de concluzii, observăm în primul rând faptul că, naturalmente, activităţile comerciale având ca obiect bunuri culturale sunt mai degrabă statice, rezervate prezenţelor *in situ,* nu atât într-un sens strict ce impun participarea activă la locul licitaţiei, cât mai ales în sens organic, juridic, cel absent fiind a fi prezent chiar de la distanţă, pentru a observa, a se înscrie, a licita, a nu greşi şi a nu revoca o intenţie care deja îl va fi părăsit cu viteza luminii. Spre deosebite de comerţul online obişnuit, piaţa obiectelor de artă nu este proprie consumatorilor, a cumpărătorilor de drept comun, ci se adresează unor persoane care sunt ţinute a-şi asuma responsabilităţi suplimentare şi eforturi multiple. Dimensiunea online a comerţului având ca obiect bunuri culturale trebuie privită mai degrabă ca un *auxilium,* ca un catalizator al pieţei curente, clasice, nu ca o piaţă în sine. Paradoxal, spre deosebire de alte pieţe online emergente şi dezirabile de bunuri comune, o piaţă online liberă a bunurilor culturale este realmente de nedorit, pentru simplul motiv că, cel puţin deocamdată, aceasta nu poate să ofere garanţii suficiente cumpărătorilor, care sunt expuşi riscului de a dobândi bunuri de o autenticitate îndoielnică, fără a avea asigurate mijloacele de a rezolvi vânzările viciate, dar mai ales pentru că mediul online, prin prisma funcţiilor sale inerente, facilitează o circulaţie necontrolată a bunurilor de patrimoniu sau susceptibile de a fi integrate în patrimoniul naţional. Experienţa ultimelor decenii a confirmat interesul intens al particularilor pentru a dobândi bunuri de patrimoniu inalienabile, de o deosebită valoare arheologică şi culturală.

Pe de altă parte, instrumentate corespunzător, mijloacele online sunt mai mult decât binevenite în desfăşurarea curentă a activităţilor specifice caselor de licitaţii de bunuri culturale. Schimburile culturale la nivel global cunosc actualmente un apogeu istoric, iar circulaţia bunurilor culturale este o realitate a prezentului şi nu este doar o realitate de ordin cultural, ci este o realitate cu implicaţii patrimoniale semnificative în domeniul investiţiilor pe termen mediu şi lung. În acest context, este de aşteptat ca persoanele interesate să fie atrase de facilităţile proprii comunicării online, iar artizanii licitaţiilor culturale să investească în perfecţionarea mijloacelor optime pentru a răspunde aşteptărilor celor dintâi. Informatizarea şi digitalizarea pieţelor de artă nu mai reprezintă elemente de noutate, însă nici nu au ajuns în *punctus terminus.*

Referinţe

Ciucă V.M., *Drept roman. Lecţiuni,* ed. a II-a, Editura Universităţii „Alexandru Ioan Cuza", Iaşi, 2014

Baias F.-A., Chelaru E., Constantinovici R., Macovei I. (coord.), *Noul Cod civil. Comentariu pe articole*, ed. a II-a. revizuită şi adăugită, Editura C.H. Beck, Bucureşti, 2014

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII SUPLIMENT 2, ŞTIINȚE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-8

Blockchain Technology and Electronic Wills

Tehnologia Blockchain şi testamentele electronice

Aniela-Flavia Ţicău-Suditu[1]

Abstract: In this study we examine the impact of information technology on inheritance law, especially in the context of drafting electronic wills. We consider it a subject of great importance, noting that, although we are unable to approach in a diverse manner the natural fact of death, we can personalize, according to our own expectations and principles, our way out of the scene. In this context, the certainty and predictability of the fulfillment of the last will dispositions are essential. Given that the writing of a traditional will has multiple limitations, we will analyze the manner in which technology offers the necessary mechanisms to fulfill exactly the dispositions of the last will. To this end, we will evaluate the implications of the Blockchain technology on the inheritance issue, examining both the shortcomings and the arguments underlying the implementation of the technology on a large scale.

Keywords: Blockchain technology; electronic wills; smart contracts; crypto-wills; inheritance law

Rezumat: În acest studiu examinăm impactul tehnologiei digitale asupra dreptului succesoral, în special în contextul redactării testamentelor electronice. Considerăm că este un subiect de mare importanţă, observând că, deşi nu suntem în măsură să abordăm într-un mod divers faptul natural al morţii, ne putem personaliza, în funcţie de propriile noastre aşteptări şi principii, ieşirea din scenă. În acest context, certitudinea şi predictibilitatea îndeplinirii dispoziţii de ultimă voinţă sunt esenţiale. Având în vedere că redactarea unui testament tradiţional are multiple limitări, vom analiza modul în care tehnologia oferă mecanismele necesare pentru a îndeplini, într-o manieră cât mai fidelă, dispoziţiile de ultimă voinţă. În acest scop, vom evalua implicaţiile tehnologiei de tip „Blockchain” în context succesoral, examinând atât deficienţele, cât şi argumentele care stau la baza implementării tehnologiei pe scară largă.

Cuvinte-cheie: tehnologia de tip Blockchain; testamente electronice; dreptul de moştenire; contracte inteligente; testamente crypto

[1] Judecător, doctorand, Academia de Studii Economice din Bucureşti, e-mail: aniela.suditu@yahoo.com.

1. Short presentation of several technologies applicable for drafting wills

Since the purpose of the legislator is to rule in an efficient manner, the tools and the legislative context must be provided in order for the law recipients to exercise accordingly their rights. In the context of succession law, *de cuius* ought to have the legal instruments to draw up a valid will.

But so far, most legislations had not regulated the electronic will hypothesis, although plenty of them have the legislative framework applicable in the digital context, for example different regulations on electronic commerce, respectively legislation on electronic signature. Obviously, there is a discrepancy within the legislative landscape. Consequently, the types of wills currently stipulated in various legislations, should be integrated, in a functional way, in a digitalized context.

It is an undeniable fact that a major part of our economy involves the digital medium. In order for it to properly function, there are centralized databases used for the interchange of digital content. Even though at a first glance it appears to be a positive feature, the centralized databases present themselves with plenty shortcomings, such as increased exposure for internet fraud or hacking maneuvers.

For the groundwork of electronic wills, several technologies have been proposed. Among them, the '*Hash*' technology, that has the objective of ensuring the digital identification of the documents. This involves a cryptographic process that can be used to certify the authenticity and validity of documents, by assigning unique characteristics to each file, using calculation algorithms. As a result, if the document is accessed, modified or copied, the algorithm indicates a new hashing value, making the document history transparent.

Another process consists in using metadata as structural information on data and presenting in detail the characteristics of some files, indicating by multiple coordinates the properties of a document.

An alternative option, the blockchain technology, is a decentralized digital register of data deposited in a network that allows them to be encrypted. Nakamoto proposed in his white paper[2] the concept of '*block chain'*, a centralized ledger system for a '*framework of coins made from digital signatures'*. Blockchain technology exchanged the conventional, centralized databases with a decentralized storing mechanism, in which the digital data can be reorganized in basic units, entitled blocks.

Blockchain technology involves decentralized, encrypted and distributed network transaction system, originally used for creating bitcoin, as an alternative to a centralized transaction system, considered cost-inefficient due to the numerous taxes and intermediaries involved. For the purposes of creating crypto wills, another technology proved appropriate, respectively the Ethereum blockchain platform, that enables smart contracts in order to execute automatically

[2] Nakamoto, Satoshi, *'Bitcoin: A Peer-to-Peer Electronic Cash System', 2009,* [Online] at https://bitcoin.org/bitcoin.pdf, accessed on 26.11.2021.

different types of rights and obligations, that are the object of miscellaneous contracts or unilateral acts. Blockchain is therefore a technology that allows the development of smart contracts. These contracts are in fact agreements that are executed automatically, through a specially designated software, the mechanism allowing the automatic management of the assets listed within the platform.

2. Steps for drawing up an electronic will via blockchain

Creating an electronic will by using Blockchain technology involves a few simple steps. To begin with, *de cuius* nominates a key custodian, whose task is to inform the system in case of the testator's death. The key custodian has to update the system of his approval regarding the task of notifying the testator's death. Even though designating a key custodian is believed to be optional, considering that the beneficiaries enlisted in the blockchain could perform the same function, it would be highly advisable, mainly due to the lack of conflict of interests.

The key custodian has two main tasks. Firstly, he has to inform the network of the death of *de cuius*, generally by adding into the blockchain the death certificate. Secondly, he has to forward the blockchain will either to a designated representative, to the competent court or to a public notary, respectively to the administrative institutions involved.

Next, after designating the key custodian, the testator records both beneficiaries and assets in the network. Afterwards, users are linked to different crypto addresses to secure the data. Users also provide details on the distribution of assets. Access to the platform could therefore be achieved by creating an account by the testator, and the validity conditions could be verified in real time by an algorithm. The will could be updated at any time and signed electronically, and the custodian platform would be its depositor in a blockchain system that would ensure a high degree of security and evidentiary facilities. Even if the content is private, any data change would automatically be flagged by the system, in order to secure the input data. In this process, it would not be necessary to appoint witnesses, lawyers or executors, since the will of the testator, as specified into the blockchain, will be executed.

Therefore, in the blockchain version, it could be used a custodian-platform recognized or approved by the state, thus vested with public power, and the proof of the validity of the will could be carried out by the notary public who would proceed with the successional execution.

However, the custodian-platform could also act as an e-will executor, verifying the inheritance options and, subsequently, proceeding directly to the transfer of the inheritance rights and obligations to the estates of the acquiring individuals, according to a well-predefined algorithm. Also, the testator can add in the blockchain a notary or witnesses that can testify[3] the testator's free will and lack of undue influence in drafting the will.

[3] This can be done by using a crypto key assigned by the testator.

On the blockchain, everything could be anonymized, including the will itself or the terms of the will, the identities of all the individuals enlisted in the blockchain, respectively the testator, the key custodian, the notary, the witnesses and the beneficiaries. The feature of anonymity is achievable from a security point of view, due to the fact that each block of the chain has imprinted in it the time of its configuration, and this information is disseminated to all nodes.

3. Comparison between traditional wills and crypto wills

It is a constantly accepted fact that drawing up wills presents various challenges, both physical and psychological, internal and external. For example, traditional holographical wills can easily be forged, hidden, destroyed or lost. They can also be misinterpreted or invalidated. Obviously, these weaknesses can and should be reduced by using the appropriate methods, such as a secure technology. First of all, the simple step of storing the will on a digitalized medium, no matter the format of encryption, provides additional assurances for the validity of the Electronic Will[4]. The feature of adjusting the will accordingly, following the user's wishes, indicates a solid advantage of the electronic will, noting that it is straightforwardly accomplished.

Without a doubt, the option of registering a will within a digitalized medium presents itself in a darker shade in case of hacking, of private information counterfeit or in the context of another type of internet fraud. Nevertheless, this can be avoided either by raising digital security, by having a hardcopy of the e-will or by accessing a technology that is better fitted for this type of legal aspect. Blockchain technology is in fact a digital register of data which is deposited on a network that enables both data encryption and the elaboration of smart contracts[5].

One particular advantage of the distributed network feature is the fact that copies of the Will are spread on various nodes. As a consequence, it would be fairly easy to detect any inconsistency between those copies, that could eventually be labeled as untrustworthy. Therefore, due to the mechanisms that it involves,

[4] We used the term 'electronic will' or 'e-will' for wills registered within a digitalized medium, and the term 'crypto will' or 'blockchain will' for a specific type of electronic will, that are registered using the blockchain technology.

[5] For a more developed scheme of Crypto-Will steps, see: Crawford, Bridget J., *Blockchain Wills*, 95 Indiana Law Journal 735 (2020), [Online] at https://ssrn.com/abstract=3346493, accessed on 26.11.2021.

The author outlines seven steps, as it follows: will coding and listing of assets and of beneficiaries, securing individuals through crypto addresses, linking through smart contracts all the third parties involved, including the financial institutions and the administrative ones; linking the will to the official records (such as death, marriage and birth databases, hospital records, etc.) and to a software that verifies the status quo of the testator, in order to double-screen his existence, automatically flagging changes of the will and, finally, automatically executing the contract through smart contracts technology, after the testator's death.

Blockchain technology is considered 'un-hackable', this feature rendering the desirability for storing data content.

Another issue ready to be solved by applying the blockchain technology in the testamentary succession legislation consists in reducing the incidence of unclaimed inheritances[6], due to the automatic execution of the will. As described in the legal literature, integrating unclaimed inheritance is a legal issue with surprisingly many repercussions, such as affecting the micro and macro-economy by not distributing the assets to the rightful beneficiaries, that leads to underdevelopment, abandonment and inequality. As a consequence, family disagreements on inheritance issues would be reduced to a minimum.

As we pointed out throughout this article, the Crypto Will has plentiful advantages in comparison to the Traditional Will[7]. Therefore, a will system based on the blockchain technology, combined with the smart contract technology, offers the best of the two digital worlds. Blockchain technology provides a chain of assets and individuals that are linked to blocks. Simultaneously, the smart contract feature enables the automatic allocation of assets to the designated individuals. The Blockchain system allows the precise recording and managing of different types of transactions or contracts, with limited or no need at all for third parties.

Though is a cost-effective technology, some argue that the Blockchain system might enhance the tax evasion and auditing[8], compared to the traditional will. Consequently, cryptocurrency in general[9] and Bitcoin, in particular, including the technology it is founded on, blockchain, are considered befitting for criminal activity[10], due to the lack of publicity and the decentralized feature of digital ledger of transactions.

From the perspective of the costs involved, the crypto will proves to be by far more accessible than the traditional will drafted by the public notary or by the attorney at law. In the legal literature, there were proposed different algorithms for calculating the cost analysis of registering and executing a will. We will exemplify

[6] Wan Nur Izzah Wan Muhamad Fokri, Engku Muhammad Tajuddin Engku Ali, Nadhirah Nordin, Wan Mohd Yusof Wan Chik, Sumayyah Abdul Aziz, Ahmad Jazlan Mat Jusoh, *The Unclaimed Inheitance Issues: a solution using Blockchain Technology*, Psychology and Education, 2021), [Online] at https://pdfs.semanticscholar.org/3dcd/9ceac044a29b8817deb9ae487b1ebefe3d61.pdf, accessed on 26.11.2021.

[7] For a broader perspective, in another article we examined, in a more detailed manner, the pros and cons of two type of wills: Electronical wills and the traditional ones: Ticau-Suditu Aniela-Flavia, Silvia Uscov, *Testamentul electronic*, Curierul Judiciar, nr. 5/2021.

[8] Walaa J. Alharthi, *Using Blockchain in WAQF, Wills and Inheritance Solutions in the Islamic System*, International Journal of Economics and Business Administration Volume IX, Issue 2, 2021 pp. 101-116.

[9] Ethereum, Dash, Litecoin, Ripple and others.

[10] See also, Shih, T.F.; Chen, C.L.; Syu, B.Y.; Deng, Y.Y. *A Cloud-Based Crime Reporting System with Identity Protection.* Symmetry 2019, pp. 255.

one such algorithm[11]. The variables considered for calculating the total amount necessary imply: the will editing, the issuing of the death certificate, the distribution of the assets enlisted in the blockchain, and the technical solutions employed, respectively the multiplication operation, the comparison operation, the hash function operation and the signature operation. To wrap it up, the authors concluded that the total communication cost was of 1280 bits, which denotes a very small rate. Therefore, the cost efficiency feature renders the blockchain technology extremely appealing.

As a consequence, making a crypto will turns out to be an accessible endeavor, pointing towards the versatile, digital limits that keep reducing themselves in order to offer the involved users a boundless experience. Drawing up a blockchain electronic will would not only be comfortable, but would also provide security guarantees.

It is an obvious fact that the formalities stipulated for the making of a traditional will, are no longer able to accomplish the purposes for which they were postulated. As a conclusion, Blockchain technology can achieve the equilibrium between maintaining the traditional wills formalities' rationale and updating the legislation to a digitalized context, suitable for our lifetime.

4. The blockchain applied to wills

Generally, the legislations that have provisions regarding electronic wills, have three common conditions. The requirement of a will drafted in a digital format and stored on a digital medium, that presents the digital or electronic signatures of the testator and witnesses. These formalities are followed by another one, that concerns the actual manner of communication, enabling the testator and witnesses, or, when needed, public notaries, to be connected through audio-visual technology, even though physically separated[12].

In this context, the '*proof of existence'* element has the same purpose as a public notary, therefore establishing not only the data ownership but also assessing the integrity and validity of the analyzed documents. It is obvious that there are plenty advantages both for the testator and for the beneficiaries in the context of creating and executing an electronic will. Additionally, having the same purpose with the electronic will stored on a regular digital platform, the crypto will, stored within a blockchain, presents plenty advantages, as examined throughout this paper, derived in particular from the distributed network structure. Therefore, it involves a will administration designed as an '*end-to-end process'*, with its main features: cryptographic, static and with a software which is both distributed and decentralized.

[11] Chen, C.-L.; Lin, C.-Y.; Chiang, M.-L.; Deng, Y.-Y.; Chen, P.; Chiu, Y.-J. *A Traceable Online Will System Based on Blockchain and Smart Contract Technology*. Symmetry 2021, 13, 466, https://doi.org/10.3390/sym13030466, accessed on 26.11.2021.

[12] Crawford Bridget J., *Blockchain Wills* (February 22, 2019). 95 Indiana Law Journal 735 (2020), [Online] at https://ssrn.com/abstract=3346493, accessed on 26.11.2021.

Even though the individuals enlisted within the Blockchain are aware about the drafted Will, they cannot open it, being a private document, accessible only by the testator' crypto address, as long as he is alive. At the moment of his demise, the will is automatically accessible to the beneficiaries. Moreover, due to its feature of being a smart contract, the will can be executed automatically.

Another interesting aspect is that only the beneficiaries can decode the addresses. As a consequence, any alteration of the Will can be observed by the individuals enlisted, who will be alerted about the action and its coordinates: time, location and crypto-address. Nevertheless, the identity of the beneficiaries is unknown to the others[13], thus reassuring the testator of the private nature of the will.

5. Using smart contracts in drawing up wills

A smart contract is an agreement based on a specifically allocated software, characterized by the automatic execution of both rights and obligations. Specifically, smart contracts[14] are self-executing, transparent, customized and accessible. They can verify and execute the provisions drafted within the will, automatically transferring the estate to the designated beneficiaries. Smart contracts[15] are distributed on networks, in order to execute different types of transactions, in case of meeting the contractual terms[16].

The option of drafting a custom-made smart contract generates the premises of an efficient and easy execution of the Will. Because it facilitates the transfer of both real and digital assets[17], drafting a crypto-will is an optimal solution specifically for the testators involved in cryptocurrency transactions, such as bitcoin or Ethereum, enabling the beneficiaries to access the testator's accounts, thus preventing the losing of various types of digital assets.

As a consequence, in this context, a smart contract consists of a mechanism specially designed in the purpose of enabling the immediate execution and

[13] Noting that every single user is given an encrypted digital signature that it is not fitting to lead towards the identification of the user linked with an elected pseudonym.

[14] See also, Buterin V., *A next-generation smart contract and decentralized application platform.* White Paper 2014, 3, 1–36; Wang, S, Ouyang L., Yuan Y., Ni X., Han, X, Wang F.Y., *Blockchain-enabled smart contracts: Architecture, applications, and future trends*, IEEE Transact. Syst. Man Cybern. Syst. 2019, 49, 2266–2277, [Online] at https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, accessed on 26.11.2021.

[15] Also called digital contracts or blockchain contracts.

[16] Sreehari P., Nandakishore M., Krishna G., Jacob J. and Shibu V. S.,*'Smart will converting the legal testament into a smart contract'*, *International Conference on Networks & Advances in Computational Technologies , NetACT*, 2017, pp. 203-207.

[17] For a perspective regarding digital assets, see Ticau-Suditu A.F., '*Digital Legacy'*, Analele Ştiinţifice Ale Universităţii Alexandru Ioan Cuza Din Iaşi, Ştiinte Juridice, vol. 3/2020, [Online] at https://heinonline.org/HOL/LandingPage?handle=hein.journals/anuaiclaw66&div=54&id=&page=, accessed on 26.11.2021.

administration of the wills and deceased' estates, following their registration within the blockchain. Accordingly, both the will itself and its content would be private, enabling only the author and its beneficiaries to access its content, due to the distinctive crypto-addresses. After the entry of the testator's death into the blockchain, the registered will is executed automatically, according to its provisions, and the role of third parties or intermediaries is either reduced or even eliminated.

6. Blockchain application

Many developers saw the potential in this technology, either through the management of bitcoin cryptocurrencies or via the use of smart contracts[18] or data science and cyber security[19]. The blockchain technology has a strong social impact and it is employed for educational or charity purposes, including by UNICEF[20], by different egalitarianist movements[21], or even by governments[22] for achieving various purposes[23].

In the legal field, the potential of smart contracts technology finds itself at a pioneering stage. Many developers offer solutions for replacing lawyers or even courts, offering the users alternatives to the traditional methods for solving cases. Such examples are the platforms *donotpay.co.uk,* that provide free legal expertise for general users, *jury.online.com,* that can be accessed by agreeing users and

[18] Di Pierro M., '*What Is the Blockchain'* in Computing in Science & Engineering, vol. 19, no. 05, pp. 92-95, 2017, [Online] at https://doi.ieeecomputersociety.org/10.1109/MCSE.2017.3421554, accessed on 26.11.2021.

[19] B. Thuraisingham, *'Blockchain Technologies and Their Applications in Data Science and Cyber Security'*, in 2020 3rd International Conference on Smart BlockChain, Zhengzhou, China, 2020 pp. 1-4.

[20] The agency launched a general invitation to help the Syrian children by crypto transactions, labeling it as '*the first humanitarian fundraising campaign',* see more, Mathias Roumy, UNICEF – Game Chaingers, *MakeMePulse,* [Online] at https://m.makemepulse.com/unicef-game-chaingers-41802cfa0b3c, accessed on 26.11.2021.

[21] See for example, https://cryptochicks.ca; https://hackernoon.com/make-way-for-the-crypto-queens-4945df6d33f, https://www.inc.com/zoe-henry/lgbt-community-launches-cryptocurrency.html, accessed on 26.11.2021.

[22] For example, see Neuberger J.D., Wai L. Choy & Dodge T. M., *Modernizing Real Estate Records with Blockchain*, THE NAT'L L.F. (2018), [Online] at https:// nationallawforum.com/2018/06/30/modernizing-real-estate-records-with-blockchain, accessed on 26.11.2021, the authors concluding that '*blockchain has the potential to improve upon problems that hamper deed recording systems in the United States today'.*

[23] For example, the Blockchain Apparatus, is an application based on blockchain technology, that uses the content data registered on an official database, such as US Social Security Administration, that gives access to the Death Master File. This application enables the possibility of a crypto will that can be executed automatically via smart contracts technology.

provides a jury that can decide small claims matters, for a minimum cost[24], and the Zweispace platform[25], having as an objective the implementation of a self-executing will system by automatically distributing an estate assets to the beneficiaries.

Even though wills are not contracts, being defined by their unilateral character, due to the fact that it involves the will of only one party, they can be executed through a blockchain - smart contracts platform. Consequently, most of the challenges encountered while executing a traditional, paper will, can be addressed through the technology employed. For example, in case of estate execution disagreements or arguments related to the will, there are plenty of applications within the Blockchain that could offer solutions, by accessing a special designed mechanism involving dispute resolution.

The legal literature concerning the blockchain technology projected a number of functional systems involving crypto wills. One such system[26] envisions the following structure: a Blockchain Center (where the will is drafted and registered by the testator, who also provides relevant data, such as personal information, passwords, accounts and other private information; the blockchain center verifies the input data, encrypting it and assigning a key and secured addresses), an applicant (the testator), beneficiaries or family (in this case, the testamentary successors; this could also include the interested parties), a competent court (in case of will applications; according to national legislations, a public notary and witnesses can be enlisted into the blockchain, with the same purpose), a hospital (issues the testator's death certificate). As we mentioned before, the applicant can also enlist into the blockchain key custodians, witnesses or public notaries, in order for a smoother execution of the will.

The impact of implementing blockchain technology in succession law, form a macro economical perspective is also analyzed by different authors. One author[27] identifies the following: reducing strict bureaucracy, enhancing transactional transparency due to the better managing the records kept via Blockchain; decreasing the corruption due to the transparency, distribution feature, the security guarantees it presents and the low costs it involves, enabling the crowdfunding for development[28] by the facility of collecting small contributions,

[24] [Online] at https://venturebeat.com/2017/10/23/jury-online-wants-to-replace-lawyers-with-blockchain-technology/, https://venturebeat.com/2017/07/12/donotpay-expands-its-free-legal-services-across-u-s-and-u-k/, accessed on 26.11.2021.

[25] [Online] at https://www.cbinsights.com/company/zweispace, accessed on 26.11.2021.

[26] Chen C.-L., Lin C.-Y., Chiang M.-L., Deng Y.-Y., Chen, P., Chiu, Y.-J., *A Traceable Online Will System Based on Blockchain and Smart Contract Technology*. Symmetry 2021, 13, 466, https://doi.org/10.3390/sym13030466, accessed on 26.11.2021.

[27] Alharthi W.J., *Using Blockchain in WAQF, Wills and Inheritance Solutions in the Islamic System*, International Journal of Economics and Business Administration Volume IX, Issue 2, 2021 pp. 101-116.

[28] See also, Zhu H. and Zhou Z. Z., '*Analysis and outlook of applications of blockchain technology to equity crowdfunding in China'*, Financial innovation, vol. 2, no. 1, p. 29, 2016.

in order to enable the founding of a major project, enhancing an ecosystem of integrated property development that could support sustainable projects, due to an inclusive system that is enabled by the blockchain technology.

7. Conclusion

Throughout this article, we outlined the importance of bringing up-to-date the legal and regulatory framework in the succession law context, in order to take advantage of the Blockchain mechanism. Our assessment on Blockchain wills convinced us that they would be more secure, easier to conclude and would display a higher rate of validity in contrast with the traditional, paper wills.

As a corollary, the option for drafting electronic wills via blockchain technology would benefit both the decedent and successors of the estate, enabling to preclude legal arguments, as it is easier to avoid the wills' misinterpretations, knowing that the Blockchain technology provides for a will that is not only unique, unalterable, secure and irreversible, but is a digital versatile object, that can be multipurposed and personalized, offering a plenary experience to composing a will, a life's last expression, in a most humane display.

Plenty concerns regarding the blockchain wills are still to be addressed so that various national legislations would be able to implement the technology. Therefore, the harmonization with the current legal framework is crucial. Nevertheless, the system could be adjusted in order to fully satisfy the present rules, bearing in mind that the obstacles for implementing the technology are mainly of an administrative nature, and not of a substantial one. For example, testators, public notaries or key custodian could attest in advance their identity, in order to facilitate the judicial successional procedure. We consider that the best way to make legal provisions regarding the use of the blockchain technology would be through a multinational regulation, for instance, the EU Regulations, that would act as a catalyst for implementing a more innovative legal approach.

Nevertheless, creating legal provisions for crypto wills is essentially a matter of society's vision. In the context of valuing the freedom of disposition above abiding the will's traditional formalities, and interpreting the law in order to be effective rather than fixed, it is an obvious choice the enacting of crypto-wills. For these reasons, we consider it necessary and opportune for the legislator to be proactive in the context of the electronic will regulations, and specifically for crypto wills, by stipulating the option of using blockchain technology as appropriate with the context of digitalization.

References

Buterin, V., *A next-generation smart contract and decentralized application platform.* White Paper 2014

Chen C.-L., Lin C.-Y., Chiang M.-L., Deng Y.-Y., Chen, P., Chiu, Y.-J., *A Traceable Online Will System Based on Blockchain and Smart Contract Technology.* Symmetry 2021, 13, 466, https://doi.org/10.3390/sym13030466

Crawford B.J., *Blockchain Wills*, 95 Indiana Law Journal 735 (2020)

Zhu H. and Zhou Z. Z., '*Analysis and outlook of applications of blockchain technology to equity crowdfunding in China*', Financial innovation, vol. 2, no. 1, 2016

Nakamoto, S., *'Bitcoin: A Peer-to-Peer Electronic Cash System'*, 2009

Neuberger, Jeffrey D., Wai L. Choy & Trevor M. Dodge, *Modernizing Real Estate Records with Blockchain*, THE NAT'L L.F. (2018)

Pierro, M. Di '*What Is the Blockchain'* in Computing in Science & Engineering, vol. 19, no. 05, 2017, https://doi.ieeecomputersociety.org/10.1109/MCSE.2017.3421554

Sreehari P., Nandakishore M., Krishna G., Jacob J. and Shibu S., *'Smart will converting the legal testament into a smart contract'*, *International Conference on Networks & Advances in Computational Technologies , NetACT*, 2017

Shih T.F., Chen C.L., Syu, B.Y., Deng Y.Y., *A Cloud-Based Crime Reporting System with Identity Protection.* Symmetry 2019

Ticau-Suditu A.F., '*Digital Legacy'*, Analele Ştiinţifice Ale Universităţi Alexandru Ioan Cuza Din Iaşi, Ştiinte Juridice, vol. 3/2020

Ticau-Suditu A.-Fl., Uscov S., '*Testamentul electronic'*, Curierul Judiciar, nr. 5/2021

Thuraisingham, B., *'Blockchain Technologies and Their Applications in Data Science and Cyber Security'*, in 2020 3rd International Conference on Smart BlockChain, Zhengzhou, China, 2020

Walaa J. Alharthi, *Using Blockchain in WAQF, Wills and Inheritance Solutions in the Islamic System*, International Journal of Economics and Business Administration Volume IX, Issue 2, 2021

Wan Nur Izzah Wan Muhamad Fokri, Engku Muhammad Tajuddin Engku Ali, Nadhirah Nordin, Wan Mohd Yusof Wan Chik, Sumayyah Abdul Aziz, Ahmad Jazlan Mat Jusoh, *The Unclaimed Inheitance Issues: a solution using Blockchain Technology,* Psychology and Education, 2021

Wang S., Ouyang L., Yuan Y., Ni, X., Han X., Wang F.Y., *Blockchain-enabled smart contracts: Architecture, applications, and future trends*, IEEE Transact. Syst. Man Cybern. Syst. 2019

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-9

Tehnologia *blockchain* în executarea contractelor de publicitate comercială *online*

Blockchain Technology in the Performance of Online Advertising Contracts

Aura-Elena Amironesei[1]

Rezumat: Relaţiile contractuale în spaţiul virtual au dobândit o nouă dimensiune amprentată inevitabil de avansul tehnologic fără precedent. Noile tehnologii tind să suplinească aportul uman în executarea contractelor, mai ales a celor cu executare de natură la rândul său virtuală, înlăturând totodată şi erorile, respectiv fraudele umane. Contractele de publicitate comercială *online* nu reprezintă o excepţie de la incidenţa neexecutărilor contractuale sau de la fraudarea părţilor prin diverse mijloace la rândul lor digitale. În acest context, noile tehnologii, în special tehnologia *blockchain*, se prefigurează drept o soluţie pentru executarea conformă a tuturor termenilor contractuali ce sunt încorporaţi într-un *smart contract*. Elementele contractuale clasice sunt transpuse în linii de cod ce devin legea părţilor în publicitatea *online*, iar criptomonedele sau *tokens* iau locul clasicului „preţ” plătit în bani.

Cuvinte-cheie: comerţ internaţional; publicitate comercială; *smart contracts*; *blockchain*

Abstract: The contractual relationships in virtual space have acquired a new dimension which is inevitably marked by the unprecedented technological advance. The new technologies tend to replace the human input in the execution of contracts, especially the ones involving a virtual performance, preventing human errors and frauds. *Online* advertising contracts do not stand as an exception from breaches of contract, neither from digital types of fraud. In this context, the new technologies, especially the *blockchain* technology, appear to be a solution for the full performance of the contractual terms that are embedded in a smart contract. The traditional contractual elements are transposed into lines of code which become the law of the parties in *online* advertising, and cryptocurrencies along with tokens become a replacement for the traditional price paid in money.

Keywords: international trade; commercial advertising; smart contracts; blockchain

[1] Doctorand, Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iaşi, e-mail: aura.amironesei@yahoo.com.

Introducere

Apariţia tehnologiei *blockchain* şi ramificarea utilizării sale în domenii din ce în ce mai variate, a condus la inovarea unor domenii tradiţionale şi a reprezentat un răspuns la multe probleme ivite din cauza factorului uman implicat în anumite mecanisme. În acest proces de extindere, domeniile marketing-ului şi dreptului nu au fost ocolite, fiind prinse la rândul lor, de curând, în curentul „*blockchain*". În cuprinsul prezentului articol vom analiza în ce mod şi de ce a fost implementată tehnologia *blockchain* în contractele de publicitate comercială *online*, ce soluţii a oferit la probleme existente în domeniu, ce elemente contractuale clasice au fost inovate şi dacă utilizarea sa reprezintă sau nu un avantaj cu perspective de viitor.

1. Premisele existenței tehnologiei blockchain în publicitatea comercială online

Pătrunderea tehnologiei *blockchain* în peisajul publicităţii *online* nu s-a realizat odată cu apariţia acesteia, ci ulterior şi treptat, având la bază o serie de factori care au determinat şi facilitat modernizarea tehnologică a contractelor de publicitate comercială *online*. Printre aceşti factori se numără expansiunea industriei publicităţii *online* şi creşterea vertiginoasă a numărului şi formelor de fraudare a mecanismului publicităţii *online*.

1.1. Expansiunea industriei publicităţii online

După extinderea utilizării internetului, a avut loc o creştere fără precedent a furnizării serviciilor de publicitate *online*[2] şi, în mod subsecvent, a veniturilor obţinute de către prestatorii de astfel de servicii, direct proporţional cu bugetele alocate acestei industrii de către profesionişti. Publicitatea în mediul virtual a devenit în timp o nouă formă de afacere larg răspândită[3], cererea pentru astfel de servicii fiind în continuă creştere şi datorită eficienţei sale crescute, în special a celei de tip personalizat[4] (*targeted advertising*[5]).

[2] European Parliament, *Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice,* Study Requested by the IMCO committee, June 2021, DOI: https://doi.org/10.2861/80 | QA-02-21-683-EN-N, [Online] la https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662913/IPOL_STU(2021)662913_EN.pdf, accesat 30.11.2021, p. 12 şi PwC, Macrotrends. Global revenue – growth by segments, [Online] la https://www.pwc.com/gx/en/industries/tmt/media/outlook/segment-findings.html, accesat 30.11.2021.

[3] Z. Pooranian, M. Conti, H. Haddadi, R. Tafazolli, *Online Advertising Security: Issues, Taxonomy, and Future Directions*, în IEEE Communications Surveys & Tutorials, vol. XX, vo. NN, XX, 2020, https://www.researchgate.net/publication/342027116_Online_Advertising_ Security_Issues_Taxonomy_and_Future_Directions, accesat 30.11.2021, p. 1.

[4] *Ibidem.*

[5] C. T. Ungureanu, *Drept international privat european in raporturi de comert international*, Editura Hamangiu, Bucureşti, 2021, p. 371.

Această expansiune, catalogată drept un *boom*[6], a ajuns să plăsmuiască un real ecosistem al publicităţii *online*, alcătuit din lanţul contractual în baza căruia serviciile specifice sunt prestate. În respectivul ecosistem regăsim toate părţile contractuale drept actori cu roluri bine definite, alături de toate acţiunile, respectiv drepturile şi obligaţiile contractuale, ce se regăsesc în cuprinsul contractelor.

Odată cu creşterea cererii şi a ofertei publicitare, ecosistemul a devenit din ce în ce mai complex, cu mai mulţi actori (în prezent pot fi până la aproximativ 23 de participanţi implicaţi[7]) şi mai multe relaţii, mecanisme şi acţiuni. Acest ecosistem trece de frontierele naţionale, manifestându-se la un nivel internaţional, în comerţul internaţional. Caracterul tranfrontalier proaspăt dobândit a generat dificultăţi la încheierea şi executarea contractelor de publicitate comercială *online*, inclusiv la nivel de plată a preţului, astfel că a fost nevoie de soluţii pentru înlăturarea impedimentelor din naşterea şi derularea relaţiei contractuale.

Complexitatea ecosistemului contractual aduce cu sine şi o serie de provocări pentru părţile principale implicate, doi profesionişti[8], şi anume *marketer/advertiser* şi *publisher*[9], între ele fiind o reţea de publicitate, cunoscută drept *ad network*[10], parte din *ad exchange*[11]. Ecosistemul are la bază un mecanism relativ simplu: un *marketer* (înţeles drept participant la comerţul internaţional care doreşte să îşi promoveze produsele prin intermediul publicităţii *online*) contractează cu un *publisher* furnizarea unor servicii de publicitate *online* (*publisher*-ul fiind cel care prestează serviciile sub diverse forme, în funcţie de obiectul contractului). După

[6] PwC, *Is blockchain the answer to digital advertising's trust gap?*, 2019, [Online] la https://www.pwc.com/us/en/industries/tmt/assets/2019-*blockchain*-in-advertising.pdf, accesat 30.11.2021, p. 2.

[7] *Ibidem*. Pentru o imagine vizuală a celor potenţial implicaţi în publicitatea *online*, a se vedea https://www.slideshare.net/tkawaja/luma-display-ad-tech-landscape-2010-1231, accesat 30.11.2021.

[8] Conform art. 3 din C. civ., un profesionist este cel care exploatează o întreprindere, acţiune definită drept *„exercitarea sistematică, de către una ori mai multe persoane, a unei activităţi organizate ce constă în producerea, administrarea sau înstrăinarea de bunuri ori în prestarea de servicii, indiferent dacă are ori nu un scop lucrativ*".

[9] Z. Pooranian, M. Conti, H. Haddadi, R. Tafazolli, *op. cit.*, p. 3.

[10] *Idem*, p. 1. Pentru mai multe detalii despre *ad network*, a se vedea, MoPub Inc., *Understanding ad networks*, 2017, [Online] la https://www.mopub.com/content/dam/mopub-aem-twitter/migration/39639-mopub-understanding-ad-networks.pdf, accesat 30.11.2021.

[11] Z. Pooranian, M. Conti, H. Haddadi, R. Tafazolli, *op. cit.*, p. 3. Pentru mai multe detalii despre *ad exchange*, a se vedea, S. Muthukrishnan, *Ad Exchanges: Research Issues*, în Leonardi S. (eds), *Internet and Network Economics*, WINE, Lecture Notes in Computer Science, vol 5929. Springer, Berlin, Heidelberg, 2009, https://doi.org/10.1007/978-3-642-10841-9_1, [Online] la http://www.eecs.harvard.edu/cs286r/courses/fall09/papers/start2.pdf, accesat 30.11.2021. Pentru mai multe detalii despre diferenţa dintre ad network şi ad exhange, a se vedea, Open X, *Ad networks vs ad exchanges: how they stack up*, 2010, [Online] la https://www.cs.princeton.edu/courses/archive/spring13/cos448/web/docs/adnets_vs_exchanges.pdf, accesat 30.11.2021.

încheierea contractului, *publisher*-ul afişează reclamele cu produsele şi/sau serviciile *marketer*-ului unui consumator. Datele obţinute din interacţiunea consumatorului cu acel conţinut publicitar afişat sunt transmise apoi, de către *publisher*, către *marketer*. În toată această construcţie contractuală, pe de o parte, *marketer*-ul trebuie să aleagă într-un mod cât mai eficient *publisher*-ul (şi, implicit, ecosistemul pentru lanţul contractual). De cealaltă parte, *publisher*-ul trebuie să atingă standardele impuse de *marketer*, să ofere informaţii cu un grad ridicat de acurateţe înapoi către *marketer*, să îndeplinească şi aşteptările consumatorilor în materie de conţinut publicitar ce le este afişat şi să asigure mecanisme de informare cu privire la prelucrarea datelor cu caracter personal.

În final, utilizarea la un nivel fără precedent a publicităţii *online*, prin diverse modalităţi de realizare a acesteia[12] (adică o multitudine de obiecte contractuale), are drept consecinţă şi dificultatea unui profesionist (*marketerul/advertiserul*) în a aprecia, în cazul în care desfăşoară o campanie publicitară extinsă pe mai multe domenii ale publicităţii *online* (*banner ads*[13], *video*[14], *influencer marketing*[15] etc.), în mod concret, care tip de publicitate este cel mai eficient şi ce conţinut publicitar a avut cel mai mare impact asupra consumatorilor[16]. În mod corelativ, din cauza aceleiaşi diversificări a instrumentelor publicitare *online*, este dificil pentru un profesionist (*marketer*) să afle dacă şi prin care tip de publicitate sau ce cocontractant (*publisher*) a încălcat prevederile legislaţiei în materie de drepturi cu caracter personal, atunci când apelează la mai multe mijloace de a realiza publicitatea *online*. Astfel de încălcări îl prejudiciază în mod cert şi direct, din moment ce reclamele sale sunt asociate cu brand-ul său[17]. Prejudiciul este mai mare atunci când consumatorii sunt cetăţeni europeni pentru că aceştia se bucură de reglementări în favoarea lor mult mai riguroase, care le conferă o protecţie sporită a datelor cu caracter personal şi care îi protejează împotriva unor practici comerciale neloiale în care publicitatea *online* este implicată.

[12] C. T. Ungureanu, *op. cit.*, pp. 369-371.

[13] European Parliament, *Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice*, ..., p. 17.

[14] *Ibidem.*

[15] Pentru mai multe detalii, a se vedea, Z. Kadekova, M. Holienčinová, *Influencer marketing as a modern phenomenon creating a new frontier of virtual opportunities* în Communication Today, no. 9, 2018, pp. 90-104, [Online] la https://www.researchgate.net/publication/329247338_Influencer_marketing_as_a_modern_phenomenon_creating_a_new_frontier_of_virtual_opportunities, accesat 30.11.2021.

[16] PwC, *Is blockchain the answer to digital advertising's trust gap?*, ..., p. 4.

[17] M. Išoraitė, *Raising Brand Awarenees Through The Internet Marketing Tools*, în Independent Journal of Management & Production (IJM&P), v. 7, n. 2, April - June 2016, DOI:https://doi.org/10.14807/ijmp.v7i2.391, [Online] la https://dialnet.unirioja.es/descarga/articulo/5680392.pdf, accesat 30.11.2021, p. 336.

1.2. Ad fraud

Având în vedere cuantumul resurselor financiare implicate în mecanismul publicităţii *online*, frauda s-a strecurat inevitabil[18] în interiorul său. Frauda este favorizată şi de lipsa de transparenţă a *ad network*, alături de complexitatea sa[19], care reprezintă o premisă pentru breşe de securitate.

În publicitatea personalizată[20], predominantă în mediul *online*, datele pe care consumatorul le furnizează din urma interacţiunii sale cu un conţinut publicitar se cuantifică drept *ad's impact*. Acestea sunt colectate de către *publisher* şi transmise către *marketer*, denumit şi *ad buyer*[21]. În baza acestor date este măsurat impactul asupra consumatorilor a serviciilor de publicitate prestate şi deseori este determinată şi valoarea contractului (cu cât rezultatele arată că reclamele au ajuns la consumatorii ideali pentru respectivele produse şi că au existat interacţiuni, chiar conversii[22] în urma reclamelor, cu atât serviciul prestat este mai valoros, respectiv mai scump).

Statisticile obţinute în urma interacţiunii consumatorilor cu reclamele au o importanţă deosebită în *performance marketing*[23], unde preţul pe care un *marketer* îl plăteşte este stabilit în funcţie de rezultate cuantificabile. Există mai multe modalităţi de a calcula preţul contractului în contractele *online* de publicitate: *cost per mille*[24], numit şi *cost per thousands*[25] (preţ fix stabilit pentru o mie de *ad impressions*); *cost per click*[26] (preţ stabilit în funcţie de numărul de click-uri); *cost per action*[27] (se stabileşte în prealabil o acţiune ce se doreşte a fi realizată de către

[18] Z. Pooranian, M. Conti, H. Haddadi, R. Tafazolli, *op. cit.*, p. 1.

[19] *Ibidem.*

[20] Pentru mai multe detalii, a se vedea, A. Bleier, M. Eisenbeiss, *Personalized Online Advertising Effectiveness: The Interplay of What, When, and Where*, July 2015, Marketing Science, 2015, DOI: https://doi.org/10.1287/mksc.2015.0930, [Online] la https://www.researchgate.net/publication/274371236_Personalized_*Online*_Advertising_Effectiveness_The_Interplay_of_What_When_and_Where, accesat 30.11.2021.

[21] PwC, *Is blockchain the answer to digital advertising's trust gap?*, ..., p. 3.

[22] Conversiile se referă la transformarea unei simple interacţiuni cu conţinutul publicitar, în decizii comerciale de a achiziţiona produsul sau serviciul promovat (transformarea unui utilizator în consumator).

[23] Acesta se referă la marketing-ul în care preţul contractelor este determinat în baza rezultatelor campaniei de marketing. Pentru mai multe detalii, a se vedea, Zeropark Blog, What Is the Difference Between CPM, CPC, CPL, CPA and Other Performance Marketing Pricing Models?, 28th of May, 2021, [Online] la https://zeropark.com/blog/difference-cpm-cpc-cpl-cpa-performance-marketing-pricing-models/, accesat 30.11.2021.

[24] [Online] la https://www.marketingterms.com/dictionary/cpm/, accesat 30.11.2021.

[25] W. Kenton, *Cost Per Thousand (CPM)*, Investopedia, October 29, 2020 [Online] la https://www.investopedia.com/terms/c/cpm.asp, accesat 30.11.2021.

[26] Pentru mai multe detalii, a se vedea, A. Jain, S. Khan, *Optimizing Cost per Click for Digital Advertising Campaigns*, în Lattice, Volume 2, Issue 2, 2021, [Online] la https://arxiv.org/pdf/2108.00747.pdf, accesat 30.11.2021, pp. 16-21.

[27] Pentru mai multe detalii, a se vedea, H. Nazerzadeh, A. Saberi, R. Vohra, *Dynamic Cost-Per-Action Mechanisms and Applications to Online Advertising*, în Internet

consumatori, iar preţul este stabilit în funcţie de numărul de acţiuni realizate – *e.g.* să acceseze site-ul profesionistului sau chiar să cumpere produsul sau serviciul promovat prin reclamă[28]); *cost per engagement*[29] (preţul este stabilit în funcţie de numărul de interacţiuni de o anumită calitate prestabilită de către advertiser – *e.g.* consumatorul care îi accesează site-ul să navigheze pe acesta cel puţin 15 secunde); *cost per conversion*[30] (preţ stabilit în funcţie de numărul de consumatori transformaţi în clienţi în urma interacţiunii cu conţinutul publicitar).

Toate variabilele în baza cărora se poate stabili calculul preţului contractului pot avea valori modificate faţă de cele reale sau autentice din cauza unor fraude extrinseci ecosistemului precum: *bots*[31], care realizează în special acţiuni de click, conducând la *click spam*; *click farms*[32], care conduc tot la *click spam*; conturi false de consumatori care realizează interacţiuni şi acţiuni; programe de calculator frauduloase; reclame plasate pe *Ghost Sites*[33] (site-uri web incorecte sau inexistente), care generează *impression spam*[34] fiindcă acel conţinut publicitar este afişat pe pagini care sunt disponibile şi pentru consumatori[35] (pagini care nu sunt vizualizate public). În cazul *click-spam*, care este parte din *click fraud*[36] (practica de a genera *click*-uri frauduloase[37]), au loc *click*-uri invalide, nelegitime. Un *click* fraudulos este acela făcut cu intenţie şi rea-credinţă, urmărind un scop ilicit, în afara cadrului contractual. Acestea pot fi făcute manual, de către oameni[38] sau automat, prin intermediul unor programe de calculator[39], numite în general

Monetization - *Online* Advertising, April 21-25, Beijing, China, 2008, [Online] la https://web.stanford.edu/~saberi/cpa.pdf, accesat 30.11.2021.

[28] N. Daswani, C. Mysen, V. Rao, S. Weis, K. Gharachorloo, S. Ghosemajumder, the Google Ad Traffic Quality Team, *Online Advertising Fraud*, 2007, [Online] la http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.2077&rep=rep1&type=pdf, accesat 30.11.2021, p. 3.

[29] Pentru mai multe detalii, a se vedea, Content Strategy Studio, *Brand Engagement in the Participation Age*, Whitepaper, February 2014, [Online] la https://think.storage.googleapis.com/docs/brand-engagement-in-participation-age_research-studies.pdf, accesat 30.11.2021.

[30] Pentru mai multe detalii, a se vedea, [Online] https://www.facebook.com/business/help/373829586327518, accesat 30.11.2021.

[31] N. Daswani, C. Mysen, V. Rao, S. Weis, K. Gharachorloo, S. Ghosemajumder, and the Google Ad Traffic Quality Team, *op. cit.*, p. 15.

[32] [Online] la https://en.wikipedia.org/wiki/Click_farm, accesat 30.11.2021.

[33] PwC, *Is blockchain the answer to digital advertising's trust gap?*, ..., p. 5. *Ghost Sites* se referă la site-uri inexistente sau incorecte, care apar la final drept site-uri viabile pentru care advertiser-ul plătește.

[34] N. Daswani, C. Mysen, V. Rao, S. Weis, K. Gharachorloo, S. Ghosemajumder, and the Google Ad Traffic Quality Team, *op. cit.*, p. 3, 8.

[35] *Idem*, p. 3.

[36] Z. Pooranian, M. Conti, H. Haddadi, R. Tafazolli, *op. cit.*, p.. 8.

[37] N. Daswani, C. Mysen, V. Rao, S. Weis, K. Gharachorloo, S. Ghosemajumder, and the Google Ad Traffic Quality Team, *op. cit.*, p. 9.

[38] *Idem*, p. 11.

[39] *Idem*, p. 9.

clickbots[40]. Indiferent de modalitate, se consideră că sunt o formă de criminalitate cibernetică[41].

O formă particulară de *click spam* este *competitor clicking*[42], care apare atunci când un concurent, direct sau indirect, dă *click*-uri pe reclamele concurentului său pentru a-l face să cheltuie mai mult din propriul buget şi pentru a diminua concurenţa. În momentul în care un profesionist interacţionează cu reclamele concurentului său, el nu este un consumator vizat, iar preţul dat pentru interacţiunile respective reprezintă în fapt o pagubă, obiectivul sumelor alocate activităţii de marketing nefiind atins. În plus, are loc în acelaşi timp şi o consumare resurselor financiare destinate acţiunilor de promovare, astfel că majoritatea consumatorilor de pe piaţa celor doi concurenţi vor vizualiza mai mult reclamele profesionistului cu un comportament neloial pentru că acestuia i-a rămas buget şi sistemului îi apare că ar fi fost deja afişate consumatorilor doar reclamele concurentului (si se atinge *target*-ul de *clicks*), rămânând să fie afişate în continuare doar cele ale primului profesionist.

Mai există, tot în sfera *click spam*, şi *publisher click inflation*[43], situaţie în care chiar *publisher*-ul dă click pe reclamele de pe propria sa pagină pentru a primi mai mulţi bani cu titlu de preţ al contractului.

Frauda poate proveni şi de la *advertiser*, nu numai de la concurenţi, terţi, alţi participanţi în ecosistemul publicitar sau de la *publisher*. O astfel de fraudă poate avea loc atunci când deşi *publisher*-ul a avut o executare conformă, *advertiser*-ul refuză plata preţului şi invocă neexecutarea contractuală[44]. De asemenea, acesta mai poate găsi şi alte metode prin care să micşoreze în mod ilicit preţul ce trebuie achitat.

În anul 2018, prejudiciul cauzat de frauda în executarea contractelor de publicitate comercială a fost de aproximativ 19 miliarde de dolari[45]. Pe termen lung, astfel de fraude se reflectă *grosso modo* în indicele ROI (*return on investment*[46]) sau, mai specific, ROMI (*return on marketing investment*[47]), care se calculează prin

[40] Z. Pooranian, M. Conti, H. Haddadi, R. Tafazolli, *op. cit.*, p. 8.

[41] *Ibidem.*

[42] N. Daswani, C. Mysen, V. Rao, S. Weis, K. Gharachorloo, S. Ghosemajumder, and the Google Ad Traffic Quality Team, *op. cit.*, p. 9.

[43] *Ibidem.*

[44] SaTT Token, *Smart Advertising Transaction Token (SaTT),* White Paper, V.6.2, 06/01/2021, [Online] la https://satt-token.com/files/ico_satt_en.pdf, accesat 30.11.2021, p. 15.

[45] PwC, *Is blockchain the answer to digital advertising's trust gap?, ...*, p. 2.

[46] M. Zamfir, M. Manea, L. Ionescu, *Return On Investment – Indicator for Measuring the Profitability of Invested Capital*, în Valahian Journal of Economic Sciences vol. 7(2), 2016, DOI: https://doi.org/10.1515/vjes-2016-0010, [Online] la https://www.researchgate.net/publication/309516326_Return_On_Investment_-_Indicator_for_Measuring_the_Profitability_of_Invested_Capital , accesat 30.11.2021, p. 80.

[47] Pentru mai multe detalii, a se vedea, https://www.marketingevolution.com/marketing-essentials/marketing-roi.

raportare la veniturile obţinute în urma unor investiţii[48] în activitatea de marketing a profesionistului. Se consideră că cel mai mare ROI este generat în prezent de publicitatea *online*, în detrimentul ROI generat de publicitatea tradiţională[49].

În publicitatea comercială *online*, în special cea de tip personalizat, *causa remota* a oricărui contract este ca reclamele (conţinutul publicitar) să fie livrate direct doar consumatorilor interesaţi (determinaţi pe baza preferinţelor lor), care au potenţialul de a interacţiona cu acel conţinut şi chiar de a fi convertiţi în consumatori (să existe o probabilitate mare de a fi realizate conversii). Totuşi, este cu adevărat dificil să fie creat un conţinut publicitar care să fie afişat cu exactitate întocmai unui consumator „perfect". Această incertitudine în privinţa atingerii scopului şi satisfacerii *causa remota*[50] are un real impact asupra preţului contractelor de publicitate comerciale, unele fiind supraevaluate. Astfel, contractele ajung să încorporeze adesea şi un element de *alea* în ceea ce priveşte executarea obligaţiilor prestatorului de servicii de publicitate *online* (*publisher*).

În cazul publicităţii comerciale *online*, un contract de publicitate comercială executat cu bună-credinţă şi integral, conform tuturor criteriilor şi standardelor contractuale stabilite, ar trebui să ducă la atingerea cauzei expuse anterior şi să genereze astfel o valoare cât mai mare a ROI[51], ceea ce ar însemna că tot conţinutul publicitar a fost livrat acelor consumatori perfecţi care au avut interacţiuni şi chiar au realizat conversii, adică au luat decizii comerciale în baza reclamelor, în sensul de a achiziţiona produsele sau serviciile promovate, generând astfel venituri profesionistului.

În plus, se observă că în ecosistemul publicitar are lor un transfer constant de „materie", materia fiind în fapt reprezentată de diverse date, în special datele cu caracter personal ale potenţialilor consumatori. Pentru executarea unui contract de publicitate comercială *online*, datele furnizate atât de către *publisher*, cât şi de alţi actori implicaţi (precum platforme *online* de intermediere sau de prelucrare a datelor cu caracter personal în scopuri publicitare) sunt constant predate de la un participant la altul, într-o manieră secvenţională, şi se poate ajunge până la peste 20 de astfel de transferuri date într-un lanţ contractual complet. La fiecare astfel de transfer, setul de date poate suferi modificări, erori, diminuări, alterări, producându-se fie rupturi în lanţul contractual, fie chiar fraude (ca urmare a erorilor sau de sine stătătoare) sau încălcări ale legislaţiei cu privire la protecţia datelor cu caracter personal. În ecosistem există participanţi întocmai cu rolul de a preveni

[48] P. Koen, D. Reibstein, *Challenges in Measuring Return on Marketing Investment: Combining Research and Practice Perspectives*, Review of Marketing Research vol. 6. Emerald Group Publishing Limited, Bingley, 2009, DOI: https://doi.org/10.1108/S1548-6435(2009)0000006009, p. 107.

[49] N. Daswani, C. Mysen, V. Rao, S. Weis, K. Gharachorloo, S. Ghosemajumder, and the Google Ad Traffic Quality Team, *op. cit.*, p. 4.

[50] C. T. Ungureanu, A. I. Toader, *Drept civil. Partea generală. Persoanele*, Editura Hamangiu, Bucureşti, 2019, p. 224.

[51] Z. Pooranian, M. Conti, H. Haddadi, R. Tafazolli, *op. cit.*, p. 4.

astfel de erori, respectiv fraude[52], făcându-l şi mai complex, dar fără a oferi o siguranţă integrală cu privire la atingerea scopului implicării lor. Lipsa de încredere cu privire la securitatea, integritatea şi corectitudinea datelor (securitate şi în sens de transfer) conduce la un comportament ezitant în privinţa distribuirii datelor, ceea ce are potenţialul de a frâna evoluţia şi densificarea contractelor de publicitate comercială.

Conceptul de *ad fraud* ar putea fi înţeles, într-o manieră extensivă, şi drept erori, inconsecvenţe sau limitări ale publicităţii *online* faţă de consumatori (o formă de neexecutare parţială sau executare neconformă a contractului de publicitate comercială). Sub umbrela acestei interpretări, s-ar regăsi drept *ad fraud* şi furnizarea unui conţinut publicitar neconcordant cu preferinţele consumatorilor şi într-o manieră abuzivă, agasantă, expunerea unor reclame cu potenţial de a frauda alegerea consumatorilor sau care încorporează elemente nelegale, reprezintă prin ele însele produsul unor fapte ilicite sau redirecţionează către site-uri sau profesionişti de neîncredere.

2. Smart contracts în publicitatea comercială online

În continuare, vom analiza emergenţa *smart contracts* în publicitatea *online*, ele fiind mijlocul prin care tehnologia *blockchain* a pătruns în sfera executării contractelor de publicitate comercială *online*.

2.1. Repere tehnice şi juridice privind smart contracts

Tehnologia *blockchain* a fost creată tocmai pentru a înregistra tranzacţii[53] într-un mod descentralizat[54] (printr-o reţea distribuită[55]), verificat[56] şi securizat, având totodată rolul şi de a le executa[57]. Prin *blockchain,* părţile unui contract pot trimite, primi şi stoca informaţii într-un sistem distribuit de tip *peer-to-peer*[58] (P2P),

[52] PwC, *Is blockchain the answer to digital advertising's trust gap?*, ..., p. 2.

[53] M. Corrales, M. Fenwick, H. Haapio, *Digital Technologies, Legal Design and the Future of the Legal Profession* în M. Corrales, M. Fenwick, H. Haapio (eds.), *Legal tech,* Smart contracts *and Blockchain,* Springer Nature Singapore Pte Ltd., 2019, p. 2.

[54] M. Atzori, I. Sistemi, *Blockchain technology and decentralized governance: Is the state still necessary?*, în Journal of Governance and Regulation 6(1), March 2017, DOI: https://doi.org/10.22495/jgr_v6_i1_p5, [Online] la https://www.researchgate.net/publication/315919685_*Blockchain*_technology_and_decentralized_governance_Is_the_state_still_necessary, accesat 30.11.2021, p. 45.

[55] R. Zhang, R. Xue, L. Liu, *Security and Privacy on Blockchain* în ACM Comput. Surv. 1, 1, Article 1, January, https://doi.org/10.1145/3316481, [Online] la https://arxiv.org/pdf/1903.07602.pdf, accesat 30.11.2021, p. 1.

[56] M. Corrales, M. Fenwick, H. Haapio, *op. cit.*, p. 3.

[57] R. Zhang, R. Xue, L. Liu, *op. cit.,* p. 3.

[58] Rawat D. B., Vijay Chaudhary V., Doku R. , *Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems*, în Journal of Cybersecurity and Privacy no. 1(1), 2021, [Online] la https://www.mdpi.com/ 2624-800X/1/1/2/pdf, accesat 30.11.2021, https://doi.org/10.3390/jcp1010002, p. 8.

aflat simultan pe mai multe computere[59]. Tranzacţiile valide sunt întregistrate succesiv[60] în *blocks* care se înlăţuiesc, formându-se un lanţ de *blocks*, adică *blockchain*. Liantul principal este reprezentat de *hash*, valoarea unică atribuită fiecărui block, care este apoi preluată în block-ul care urmează după şi cu care se înlănţuieşte[61]. Fiind descentralizat, *blockchain* nu se află sub controlul unei singure persoane[62], ceea ce reprezintă un avantaj, aspect pe care îl vom discuta în continuare.

Un tip de tranzacţii ce pot fi „înregistrate" folosind tehnologia *blockchain* sunt *smart contracts*. Fiind construite în baza acestei tehnologii, ajung să împrumute o serie din caracteristicile sale, rezultând o formă mai complexă decât *smart contracts* clasice. Acestea au la bază algoritmi şi presupun executarea contractelor de natură comercială[63], fără intervenţia umană, în mod automat, în conformitate cu clauzele contractuale convenite (cuprinse în codul algoritmului).

Diferenţa între *smart contracts* şi *online contracts* (cele de tip *click-wrap*[64]) constă nu numai în modalitatea de încheiere, ci şi în însăşi executarea contractului. În timp ce *online contracts* cuprind doar prevederile contractuale, fără a primi date cu privire la executarea contactului şi fără a verifica încălcările obligaţiilor contractuale, *smart contracts* se execută automat, având acces la informaţii cu privire la modul de executare a prevederilor contractuale cuprinse în codul algoritmului[65].

Smart contracts sunt imuabile[66] şi irevocabile[67], ceea ce înseamnă că este exclusă încheierea unor acte adiţionale sau modificarea lor ulterioară. În momentul în care a fost greşit codul unui contract, se poate crea alt contract în care să intre aceleaşi părţi. *Smart contracts* nu pot fi alterate, falsificate şi nici şterse[68], rămânând mereu înregistrate în acelaşi *block* (*blockchain* funcţionează şi ca o arhivă de contracte[69]), ceea ce contribuie la creşterea gradului de încredere[70] şi la asigurarea unui înalt nivel de transparenţă contractuală[71].

---

[59] D. Jaina, M. K. Dashb, A. Kumarc, S. Luthra, *How is Blockchain used in marketing: A review and research agenda*, în International Journal of Information Management Data Insights, https://doi.org/10.1016/j.jjimei.2021.100044, [Online] la https://www.sciencedirect.com/science/article/pii/S2667096821000379, accesat 30.11.2021, p. 2.

[60] M. Corrales, M. Fenwick, H. Haapio, *op. cit.*, p. 3.

[61] R. Zhang, R. Xue, L. Liu, *op. cit.*, p. 3.

[62] *Ibidem.*

[63] *Idem*, p. 5.

[64] C. T. Ungureanu, *Dreptul comerțului internațional*, Editura Hamangiu, București, 2018, pp. 160-161.

[65] M. Corrales, M. Fenwick, H. Haapio, *op. cit.*, p. 20.

[66] D. Jaina, M. K. Dashb, A. Kumarc, S. Luthra, *op. cit.*, p. 1.

[67] M. Corrales, M. Fenwick, H. Haapio, *op. cit.*, p. 23.

[68] *Idem*, p. 3.

[69] R. Zhang, R. Xue, L. Liu, *op. cit.*, p. 3.

[70] M. Corrales, M. Fenwick, H. Haapio, *op. cit.*, p. 3.

[71] *Idem*, p. 4.

Prin intermediul lor, liniile de cod[72] devin legea părţilor, iar principiul obligativităţii (*pacta sunt servanda*), care este specific şi materiei contractelor comerciale internaţionale[73], şi cel al relativităţii, devin ambele inerente executării contractuale (odată intrat într-un astfel de contract, nu se mai poate ieşi).

Validitatea unui *smart contract* nu depinde de prevederile Codului civil[74], ci de un *consensus*[75] din partea celor implicaţi în reţea[76], acesta fiind de tip *proof of work*[77] sau o validare în cazul utilizării *proof of stake*[78] (ambele sunt mecanisme stabilite pentru verificarea şi acceptarea în *blockchain* a tranzacţiilor).

Un minus pe care *smart contracts* îl prezintă este că nu oferă confidenţialitate – au caracterul de a fi *distributed*, împrumutat de la tehnologia *blockchain* pe care o utilizează. Prin urmare, toate calculatoarele din reţeaua P2P pe care se regăsesc *blocks* pot vedea contractul şi cum au participat părţile la acel contract (sunt publice[79], vizibile pentru toată lumea). Este adevărat că părţile din *smart contracts* au un pseudonim asociat, dar se susţine că în cazuri rare identitatea reală poate fi descoperită[80].

Există avansată în doctrina de dreptul comerţului internaţional concepţia „autocraţiei contractuale”[81], care presupune că un contract poate exista fără a avea aleasă o anumită lege aplicabilă, fiind o formă de autoreglementare şi autosuficienţă – contractul fiind suficient prin el însuşi pentru a fi eficace, a produce efecte juridice[82]. Concepţia nu a fost bine-primită în doctrina internaţională, opunându-i-se atât art. 3 alin. (1) şi (3) din Regulamentul Roma I[83], cât şi imposibilitatea de sine stătătoare de a exista un „contract fără lege”[84]. Luând în

[72] *Idem*, p. 20.

[73] L. Tuleaşcă, *Dreptul comerțului internațional. Tranzacții comerciale internaționale*, Editura Universul Juridic, București, 2017, p. 249.

[74] Legea nr. 287 din 17 iulie 2009 privind Codul civil publicată în Monitorul Oficial nr. 505 din 15 iulie 2011.

[75] R. Zhang, R. Xue, L. Liu, *op. cit.*, p. 3.

[76] *Idem*, p. 3.

[77] Pentru mai multe detalii, a se vedea, S. Seang, D. Torre, *Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies*, GREDEG Working Papers 2019-24, Groupe de REcherche en Droit, Economie, Gestion (GREDEG CNRS), Université Côte d'Azur, France, [Online] la https://gdre-scpo-aix.sciencesconf.org/195470/document, accesat 30.11.2021.

[78] Pentru mai multe detalii, a se vedea, S. Seang, D. Torre, *op. cit.*

[79] Innovation Lab (IDB Lab) of the Inter-American Development Bank, *Cross-Border Payments with Blockchain*, 2021, [Online] la https://publications.iadb.org/publications/english/document/Cross-Border-Payments-with-*Blockchain*.pdf, accesat 30.11.2021, p. 12.

[80] Innovation Lab (IDB Lab) of the Inter-American Development Bank, *Cross-Border Payments with Blockchain*, ..., p. 13.

[81] L. Tuleaşcă, *op. cit.*, p. 233.

[82] *Ibidem.*

[83] Regulamentul (CE) nr. 593/2008 Al Parlamentului European şi al Consiliului din 17 iunie 2008 privind legea aplicabilă obligațiilor contractuale (Roma I), publicat în JO L 177, 4.7.2008.

[84] *Ibidem.*

considerare caracterul autonom al *smart contracts*[85], acestea ar putea valida existenţa unei autocraţii contractuale.

În cazul *smart contracts*, nu există neexecutare în sensul Codului civil (nu poate fi invocată excepţia de neexecutare sau executarea neconformă), ceea ce atrage lipsa unor incidente de natură litigioasă. O discuţie pe care *smart contracts* o pot ridica este existenţa sau nu a unui caracter adezionar, dar vom lăsa acest subiect pentru o lucrare viitoare.

2.2. Utilizarea smart contracts în publicitatea comercială online

Printre utilizările tehnologiei *blockchain* de până în prezent, se numără *marketing*-ul şi, în special, publicitatea comercială *online*[86]. Având în vedere particularitatea domeniului, *smart contracts* în publicitatea *online* comportă o serie de caracteristici proprii.

Pentru început, în considerarea fluxului de date care circulă între participanţii la ecosistemul publicitar, executarea unor contracte de publicitate comercială încheiate sub formă de *smart contracts* implică primirea tuturor informaţiilor necesare şi transmiterea lor. Prin urmare, aceste *smart contracts* specifice presupun utilizarea unor instrumente ce ţin de *data analytics*[87], atât pentru furnizarea informaţiilor legate de consumatori (pentru publicitatea personalizată), cât şi pentru a obţine informaţii cu privire la rezultatele concrete ale publicităţii, în funcţie de care se stabileşte şi plăteşte automat preţul contractului. Pentru a se obţine date din afara sistemului *blockchain*, în special pentru verificarea executării contractuale, se pot utiliza *oracles*[88] create special pentru publicitatea *online*[89].

Aceste contracte ar fi afectate de o condiţie suspensivă (prealabilă[90]) constând în atingerea performanţelor (rezultatelor) specificate în contractul de publicitate comercială *online*. Numai ulterior verificării, prin intermediul datelor

[85] M. Corrales, M. Fenwick, H. Haapio, *op. cit.*, p. 18.

[86] D. Jaina, M. K. Dashb, A. Kumarc, S. Luthra, *op. cit.*, pp. 1, 2.

[87] *Idem*, p. 12.

[88] K. Mammadzada, F. Milani, M. Iqbal, L. García-Bañuelos, *Blockchain Oracles: A Framework for Blockchain-Based Applications*, în Business Process Management: Blockchain and Robotic Process Automation Forum, BPM 2020 Blockchain and RPA Forum, Seville, Spain, September 13–18, 2020, Proceedings (pp.19-34), DOI:10.1007/978-3-030-58779-6_2, [Online] la https://www.researchgate.net/ publication/344079826_Blockchain_Oracles_ A_Framework_for_Blockchain-Based_Applications, accesat 30.11.2021, p. 3. *Oracles* se referă în esență la servicii de tip *third-party* (părți „străine" de *smart contract*) care preiau informații din exterior (din viața reală) și le transmit în rețeaua *blockchain*. Acestea pot fi inclusiv aplicații software care „culeg" informații. Pentru mai multe detalii despre definiția *oracles*, a se vedea, [Online] https://en.wikipedia.org/wiki/Blockchain_oracle, accesat 30.11.2021.

[89] [Online] la https://www.coindesk.com/business/2021/09/23/umbrella-network-acquires-digital-advertising-oracle-lucidity-for-tens-of-millions/, https://tech.eu/features/20836/unboxed-brings-*blockchain*-oracles-to-aid-the-social-media-marketing-industry/ și https://www.newsbtc.com/sponsored/satt-project-offers-smart-contracts-oracles-digital-ads/, accesat 30.11.2021.

[90] L. Tuleaşcă, *op. cit.*, p. 261.

oferite de *oracles*, se poate face plata. Realizarea condiţiei nu ar avea efectul retroactiv din dreptul naţional[91], ci efectul *ex nunc* prevăzut drept regulă în Principiile Unidroit[92]. În contractele din comerţul internaţional, constatarea îndeplinirii condiţiei se realizează frecvent prin procedura de „*closing*"[93], atunci când este prevăzută o dată limită pentru îndeplinirea condiţiei şi părţile se întâlnesc la acea dată pentru a constata sau nu îndeplinirea ei. Într-un smart contract, realizarea condiţiei va conduce automat la plata preţului, fără intervenţia a părţilor contractante.

În plus, prin utilizarea tehnologiei *blockchain* se pot elimina intermediarii de care părţile depind în realizarea plăţii contractului de publicitate încheiat între ele[94]. Un astfel de intermediar poate întârzia plata contractului, poate face greşeli de calcul a preţului sau chiar modifica intenţionat statisticile în baza cărora preţul este stabilit[95] şi poate săvârşi alte tipuri de fraude. În schimb, ceilalţi intermediari specifici ecosistemului publicitar (cei care fac parte din *ad network* sau *ad exchange*) nu pot fi excluşi din *smart contracts*, o parte din ei fiind de esenţa mecanismului publicităţii *online*. Particularitatea tehnologiei *blockchain* în contractele de publicitate comercială este că *smart contracts* se încheie, pe rând, între toate părţile din întreg lanţul contractual publicitar[96]. Totuşi, se susţine că prin intermediul *smart contracts* se pot înlătura anumiţi intermediari (pentru o optimizare a numărului şi rolului lor) şi se poate facilita şi o relaţie contractuală directă între *publisher* şi *advertiser*[97].

În final, legat de imposibilitatea existenţei unei excepţii de neexecutare, există şi opinia conform căreia reţeaua *blockchain* ar opera inclusiv drept o garanţie a executării conforme a contractului[98], mai ales în publicitatea comercială *online*, unde fraudele sunt frecvente, iar executările neconforme nu pot fi în mod tradiţional verificate şi sancţionate.

[91] Art. 1.407 C. civ.

[92] Art. 5.3.2. din Principiile Unidroit, [Online] la https://www.unidroit.org/instruments/commercial-contracts/unidroit-principles-2016/, accesat 30.11.2021.

[93] L. Tuleaşcă, *op. cit.*, p. 262.

[94] M. Corrales, M. Fenwick, H. Haapio, *op. cit.*, p. 5.

[95] SaTT Token, *Smart Advertising Transaction Token (SaTT),* White Paper, p. 15.

[96] TATA Consulting Services, *Digital Advertising, Blockchain(ed),* White Paper, 2017, [Online] la https://www.tcs.com/content/dam/tcs/pdf/Industries/hitech/ abstract/Using-*Blockchain*-Digital-Ad-Ecosystem-0817-1.pdf, accesat 30.11.2021, p. 3.

[97] TATA Consulting Services, *Digital Advertising, Blockchain(ed),* ..., p. 4.

[98] M. Corrales, M. Fenwick, H. Haapio, *op. cit.*, p. 5.

2.3. Criptomonede drept „preţ" în smart contracts în publicitatea online. Studiu de caz: Smart Advertising Transaction Token (SaTT)

Plata în *smart contracts* realizate pe o infrastructură de *blockchain* poate fi făcută şi în *digital tokens*[99] (care, prin natura lor, exclud banii[100]). Prin urmare, în aceste contracte poate exista un preţ stabilit în *digital tokens*[101], acestea având o valoare proprie şi o utilitate mai extinsă decât criptomonedele[102].

În opinia noastră, *digital tokens* creează un mediu propice pentru comerţul internaţional întrucât favorizează plăţile transfrontaliere prin eliminarea diferenţelor de curs valutar (ele nu se raportează la nicio monedă[103] naţională sau regională), rapiditatea transferului, reducerea taxelor şi a comisioanelor[104] interbancare. Existând în prezent un *digital token* creat special pentru contractele de publicitate comercială *online*, se conturează premisele creşterii încheierii unor contracte internaţionale de publicitate comercială *online* şi pătrunderea acestora într-o proporţie din ce în ce mai mare în comerţul internaţional.

Acel *digital token* creat special pentru plata preţului în contractele de publicitate comercială *online* este *Smart Advertising Transaction Token*[105] (SaTT). Acesta este un *digital token* care are la bază tehnologia *blockchain*, fiind creat pe

[99] Invao, *Token Classes Explained: Coin vs. Utility Token vs. Security Token*, [Online] la https://invao.org/token-classes-explained-coin-vs-utility-token-vs-security-token/, accesat 30.11.2021.

[100] Inland Revenue Authority of Singapore, *Digital Payment Tokens*, [Online] la https://www.iras.gov.sg/taxes/goods-services-tax-(gst)/specific-business-sectors/digital-payment-tokens, accesat 30.11.2021.

[101] *Digital tokens* se referă la un echivalent digital al unui drept sau al unei valori. Un *digital token* poate reprezenta un drept de proprietate, poate oferi dreptul la anumite servicii sau poate reprezenta un mijloc de plată sau de schimb.

Pentru mai multe detalii, a se vedea, ING Bank, European Central Bank, *Cryptocurrencies and tokens*, September 2018, [Online] la https://www.ecb.europa.eu/paym/groups/pdf/fxcg/2018/20180906/Item_2a_-_Cryptocurrencies_and_tokens.pdf, accesat 30.11.2021, p. 5; https://uk.practicallaw.thomsonreuters.com/w-024-0323?originationContext=knowHow&transitionType=KnowHowItem&contextData=(sc.Default)&firstPage=true, accesat 30.11.2021.

[102] Criptomonedele sunt *digital tokens*, dar cu o utilitate restrânsă, ele stocând o anumită valoare și fiind utilizate în principal pentru plăți (nu și pentru a obține un serviciu sau pentru a oferi reprezentarea digitală a unui drept de proprietate). Pentru mai multe detalii, a se vedea, ING Bank, European Central Bank, *Cryptocurrencies and tokens*, ..., p. 5.

[103] Inland Revenue Authority of Singapore, *Digital Payment Tokens*, [Online] la https://www.iras.gov.sg/taxes/goods-services-tax-(gst)/specific-business-sectors/digital-payment-tokens, accesat 30.11.2021.

[104] Innovation Lab (IDB Lab) of the Inter-American Development Bank, *Cross-Border Payments with Blockchain*, ...

[105] Pentru mai multe detalii, a se vedea, [Online] https://satt-token.com/, accesat 30.11.2021.

reţeaua Ethereum[106] (tranzacţiile fiind înregistrate în *blocks* înlănţuite în aceasta) datorită costurilor reduse şi a rapidităţii în executare[107].

SaTT este reglementat de un *smart contract* (*SaTT Smart Contract*), care cuprinde clauzele contractului de publicitate *online*, stabilind standardele contractuale ce trebuie atinse şi remuneraţia cuvenită, care este totodată şi garantată[108]. În *SaTT Smart contracts*, plata se realizează doar dacă sunt îndeplinite condiţiile stabilite de *advertiser* şi sunt atinse rezultatele. *Advertiser*-ul poate stabili inclusiv criterii ce ţin de vârsta, sexul, domiciliul, interesul utilizatorilor cărora le sunt afişate reclamele. De asemenea, el stabileşte şi caracteristicile pe care şi le doreşte pentru cocontractantul său (poate stabili, spre exemplu, un anumit nivel de influenţă pe care acesta să îl aibă)[109].

Ulterior, rezultatele executării contractului sunt furnizate drept informaţie în *blockchain*, prin intermediul *oracles*, care pot fi stabilite chiar de către *advertiser* prin alegerea unor anumite aplicaţii[110] (spre exemplu, dacă o campanie publicitară de tip *influencer marketing*[111] are loc pe Instagram, se poate alege o aplicaţie care măsoară performanţele acţiunilor publicitare pe Instagram). Ulterior primirii informaţiei şi verificării executării contractului, preţul pentru prestarea serviciului de publicitate *online* este eliberat (transferat) *publisher*-ului[112].

SaTT poate fi folosit nu numai de *publishers* şi *advertisers*, dar şi de alţi actori implicaţi în publicitatea *online*, precum influencerii[113]. Se pot încheia *smart contracts* cu influencerii, acestea funcţionând în baza aceluiaşi mecanism. În fapt, SaTT a fost creat în mod special pentru creatori de conţinut[114] precum influencerii. Caracterul descentralizat al tehnologiei *blockchain* este unul dintre avantajele oferite de utilizarea SaTT întrucât părţile implicate în contract nu trebuie să îşi acorde toată încrederea unei agenţii de publicitate, care deţine în mod exclusiv controlul şi înştiinţează ambele părţi în limita informaţiilor pe care doreşte să le furnizeze.

---

[106] Pentru mai multe detalii, a se vedea, [Online] https://ethereum.org/en/whitepaper/ #token-systems, accesat 30.11.2021.

[107] SaTT Token, *Smart Advertising Transaction Token (SaTT)*, White Paper, p. 4.

[108] SaTT Token, *Smart Advertising Transaction Token (SaTT)*, White Paper p. 4.

[109] SaTT Token, *Smart Advertising Transaction Token (SaTT)*, White Paper p. 13.

[110] SaTT Token, *Smart Advertising Transaction Token (SaTT)*, White Paper p. 14.

[111] Z. Kadekova, M. Holienčinová, *op. cit.*

[112] SaTT Token, *Smart Advertising Transaction Token (SaTT)*, White Paper p. 13.

[113] Influencerii sunt acele persoane care au potențialul de a crea *engagement*, de a stimula conversația și/sau influența decizia de a cumpăra produse/servicii pentru un public țintă. Pentru mai multe detalii, a se vedea, IAB Romania, 2Performant, Consiliul Român pentru Publicitate, *Cod de bune practici în influencer marketing*, România, 2020, [Online] la https://drive.google.com/file/d/1ibPvEqUn9CtiFlo9Dc9e4iVobk rzSBxW/view, accesat 30.11.2021, p. 8.

[114] [Online] la https://satt-token.com/blog/2021/09/23/satt-documentation/, accesat 30.11.2021.

SaTT poate fi achiziţionat cu bani sau criptomonede şi, în mod simetric, poate fi transformat în bani sau în criptomonede sau poate fi utilizat pentru achiziţia unor produse[115], fiind ţinut într-un portofel digital[116].

Totuşi, utilizarea SaTT nu este lipsită de riscuri, cel mai mare fiind acela al existenţei şi tranzacţionării sale pe o piaţă nereglementată din punct de vedere legal, deşi la nivelul Uniunii Europene se fac paşi importanţi şi susţinuţi în această direcţie[117]. În pofida lipsei reglementării, având în vedere că operaţiunile ce implică SaTT sunt bazate pe tehnologia *blockchain*, riscul ivirii unor litigii ar trebui să fie aproape non-existent[118].

Un alt risc presupus de utilizarea SaTT este dat de dinamica şi volatilitatea[119] sa în raport cu monedele clasice. În concret, am putea ajunge să ne întrebăm dacă astfel de contracte ar putea fi calificate drept aleatorii, întrucât poate avea loc oricând o depreciere radicală a valorii – la momentul încheierii contractului să stabilit fie un anumit număr fix de SaTT, cu o anumită valoare totală, iar până la executarea sa şi momentul plăţii, deşi numărul de SaTT este acelaşi, valoarea lor să fie diminuată de câteva ori, chiar aproape de 0. O soluţie la care ne-am gândit momentan ar fi *oracles* care să furnizeze informaţii cu privire la flunctuaţia valorii, iar în baza acestor informaţii, algoritmul să adapteze numărul de digital tokens în funcţie de o valoare stabilită iniţial în contract prin raportare la o anumită monedă (o formă de clauză de indexare a preţului contractului sau clauză de adaptare[120] specifică contractelor de comerţ internaţional). Criptomonedele, o formă de *digital tokens*, fac în prezent obiectul speculei[121], ceea ce confirmă riscul expus.

2.4. Executarea contractului. Rolul tehnologiei blockchain

S-a apelat la utilizarea tehnologiei *blockchain* în publicitatea *online* pentru a asigura securitatea şi integritatea datelor în timpul executării contractului, precum şi pentru a efectua cu rapiditate şi în mod corect plata, care este verificată[122] şi făcută numai după executarea conformă a contractului.

---

[115] SaTT Token, *Smart Advertising Transaction Token (SaTT),* White Paper p. 22.

[116] Pentru mai multe detalii, a se vedea, [Online] https://satt-token.com/blog/2021/02/19/tutorial-download-trust-wallet-and-export-your-satt-erc20-wallet/, accesat 30.11.2021.

[117] Token Alliance, Chamber of Digital Commerce, *Understanding Digital Tokens. Legal Landscapes Governing Digital Tokens in the European Union,* May 2021, [Online] la https://4actl02jlq5u2o7ouq1ymaad-wpengine.netdna-ssl.com/wp-content/uploads/2021/05/Legal-Landscapes-Governing-Digital-Tokens-in-the-European-Union.pdf, accesat 30.11.2021.

[118] SaTT Token, *Smart Advertising Transaction Token (SaTT),* White Paper p. 32.

[119] SaTT Token, *Smart Advertising Transaction Token (SaTT),* White Paper p. 32.

[120] L. Tuleaşcă, *op. cit.*, p. 264.

[121] J. Silberholz. S. M. Ross, Di (A.) Wu, *Measuring Utility and Speculation in Blockchain Tokens*, September 1, 2021, http://dx.doi.org/10.2139/ssrn.3915269, [Online] la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3915269, accesat 30.11.2021, p. 2.

[122] SaTT Token, *Smart Advertising Transaction Token (SaTT),* White Paper p. 4.

Pentru executarea contractului, o etapă importantă este *consensus mechanism*[123]. Acesta reprezintă un algoritm, poate fi de tip *proof of work* sau *proof of stake* (v. supra), iar prin intermediul său se verifică dacă obligaţia a fost executată astfel cum s-a specificat contractual (dacă reclamele au fost afişate în spaţiile *online* unde s-a stabilit şi dacă afişarea a fost făcută unor consumatori cu anumite specificaţii, cu o anumită valoare sau chiar unor consumatori care au interacţionat cu conţinutul). Dacă în urma verificării reiese că executarea a fost conformă, datele vor fi înregistrate în *block*. Dacă nu, va fi ca şi cum nu ar fi fost niciodată executată obligaţia, iar plata nu va fi realizată.

Astfel cum am arătat, preţul ar fi stabilit drept o formulă[124] în contractele de publicitate comercială *online*. Conţinutul său implică variabile constând în rezultatele pe care reclamele le au. Aceste date sunt obţinute prin intermediul *oracles,* care furnizează doar date reale, autentice, cu privire la performanţele reclamelor (fiind excluse *ad frauds*). Datele oferite de *oracles* au un rol important şi în verificarea executării contractuale conforme.

De îndată ce executarea este verificată şi se califică drept conformă, plata se realizează automat, rapid, în baza calculului efectuat. Astfel, orice neînţelegere sau chiar litigiu cu privire la neexecutările contractuale, în special cele referitoare la plata preţului, ar deveni de domeniul trecutului[125] cu ajutorul *smart contracts*.

Toate datele cu privire la executare sau necesare executării (mai ales rezultatele reclamelor) sunt stocate într-o manieră ce asigură integralitatea şi securitatea lor, existând posibilitatea de a fi accesate şi verificate ulterior, fără a le afecta.

2.5. Avantajele şi dezavantajele utilizării tehnologiei blockchain

Pentru început, publicitatea *online* are rolul de a susţine *e-commerce*[126], astfel că orice element care vine spre a încuraja şi facilita încheierea şi executarea contractelor de publicitate comercială *online*, reprezintă şi un impuls pentru comerţul *online*. În cele ce urmează, vom arăta că utilizarea tehnologiei *blockchain* în publicitatea comercială *online* se prefigurează drept un suport contractual eficient şi benefic încheierii şi executării contractelor.

În primul rând, tehnologia *blockchain* preîntâmpină frauda în publicitatea *online*[127], ceea ce conduce la o reducere a prejudiciilor suferite de către profesioniştii ale căror produse sunt promovate prin publicitatea *online*. Aceasta este prin ea însăşi un simbol al încrederii, ceea ce exclude *ab initio* forme de înşelăciune/fraudă, sub toate „impersonările" sale expuse într-o secţiune precedentă.

---

[123] B. Lashkari, P. Musilek, *A Comprehensive Review of Blockchain Consensus Mechanisms*, în IEEE Access PP(99): 1-1, DOI: https://doi.org/10.1109/ACCESS.2021.3065880, [Online] la https://www.researchgate.net/publication/350031088_A_Comprehensive_Review_of_*Blockchain*_Consensus_Mechanisms, accesat 30.11.2021, p. 3.

[124] PwC, *Is blockchain the answer to digital advertising's trust gap?, ...*, p. 5.

[125] PwC, *Is blockchain the answer to digital advertising's trust gap?, ...*, p. 5.

[126] D. Jaina, M. K. Dashb, A. Kumarc, S. Luthra, *op. cit.*, p. 8.

[127] *Idem*, p. 11.

Acţiunile boţilor şi folosirea *click farms* ar fi preîntâmpinate[128]. De asemenea, tehnologia *blockchain* poate urmări digital locaţia afişării unei reclame şi verifica legitimitatea site-ului în cauză[129].

Tehnologia *blockchain* contribuie şi la eficientizarea prestării serviciilor de publicitate *online*, întrucât implică utilizarea unor date obţinute în timp real, date de încredere, iar în baza acestora consumatorii din mediul *online* ar fi expuşi unor reclame cu un grad mai mare de relevanţă pentru ei, bucurându-se în acelaşi timp şi de un grad ridicat de protecţie a datelor cu caracter personal[130]. De asemenea, şi un content creator implicat în campania publicitară poate alege campaniile potrivite pentru el, cele mai relevante şi profitabile[131] şi e sigur că dacă execută contractul conform specificaţiilor, va primi plata integrală fără întârzieri nejustificate.

Întregul ecosistem devine mai simplu, transparent şi rapid[132], executarea contractelor prin tehnologia *blockchain* realizându-se non-stop[133]. Orice fel de breşă de securitate a datelor este aproape imposibilă atunci când se utilizează această tehnologie[134]. În plus, *blockchain* acţionează şi la nivelul încrederii consumatorilor[135], asigurând creşterea sa.

Apelarea la *blockchain* reduce costurile totale ale contractelor care erau încheiate prin intermediari[136] bancari, dar adesea sunt percepute comisioane de către cei care administrează reţeaua (o formă de remuneraţie pentru utilizarea infrastructurii *blockchain*). La nivel probatoriu, datorită caracterului imuabil, irevocabil şi permament, *smart contracts* fac dovada atât a contractului, cât şi a plăţii[137], ele fiind uşor de idenfiticat prin *hash*-ul *block*-ului[138].

În final, tot în privinţa avantajelor, informaţiile generate de tranzacţii sunt vizibile doar persoanelor care au acces în blocks, ceea ce înseamnă că sunt protejate împotriva accesului neautorizat sau activităţilor ilicite, dar îşi păstrează totodată şi caracterul public faţă de ceilelalte părţi din *blockchain* (ceea ce contribuie la un anumit grad de transparenţă).

Cu privire la dezavantaje, din punct de vedere al prevederilor Regulamentului general privind protecţia datelor[139], tehnologia *blockchain*, în special cea

[128] PwC, *Is blockchain the answer to digital advertising's trust gap?*, ..., p. 5.

[129] *Ibidem.*

[130] *Idem*, p. 2.

[131] SaTT Token, *Smart Advertising Transaction Token (SaTT),* White Paper p. 19.

[132] PwC, *Is blockchain the answer to digital advertising's trust gap?*, ..., p. 5.

[133] M. Corrales, M. Fenwick, H. Haapio, *op. cit.*, p. 5.

[134] PwC, *Is blockchain the answer to digital advertising's trust gap?*, ..., p. 5.

[135] D. Jaina, M. K. Dashb, A. Kumarc, S. Luthra, *op. cit.*, p. 12.

[136] M. Corrales, M. Fenwick, H. Haapio, *op. cit.*, p. 5.

[137] Innovation Lab (IDB Lab) of the Inter-American Development Bank, *Cross-Border Payments with Blockchain*, ..., p. 48.

[138] D. Jaina, M. K. Dashb, A. Kumarc, S. Luthra, *op. cit.,* p. 2.

[139] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei

publică[140], nu îndeplineşte integral condiţiile de prelucrare a datelor cu caracter personal impuse de acesta, mai ales în ceea ce priveşte reducerea la minimum a datelor, limitarea perioadei de stocare şi principiul exactităţii, întrucât datele sunt stocate pe o perioadă nelimitată[141], iar dacă sunt incomplete sau incorecte nu pot fi modificate etc.

Deşi securitatea contractuală este garantată, securitatea infrastructurii *blockchain* nu are o siguranţă de 100%, existând o încercare de fraudă şi în 2018[142]. Nefiind reglementat, nici în zona Uniuniii Europene[143], existenţa unor fraude sau erori în *blockchain* nu ar putea fi reparate prin tragerea la răspundere şi repararea prejudiciului. Riscurile provin din faptul că încă nu se cunosc toate implicaţiile juridice.

Un ultim dezavantaj este reprezentat de lipsa standadizării în materie de plată[144].

Concluzii

Automatizarea executării contractuale este specifică noilor tehnologii care îşi fac simţită prezenţa în domeniul juridic. Pe măsură ce acestea sunt dezvoltate, aplicabilitatea lor va deveni din ce mai extinsă, peisajul juridic urmând a fi profund transformat. Parte din noile tehnologii este şi *blockchain*-ul, care se prefigurează drept un mijloc de modernizare, eficientizare, securizare şi transparentizare a ecosistemului publicitar. Fiind deja implementată, deşi nu la scară largă, aceasta pare să fi avut succes până în prezent, întrucât în urma unei lungi şi detaliate analize a doctrinei existente, nu am regăsit a fi ridicate probleme din practică în legătură cu *smart contracts* în publicitatea comercială *online*.

Tehnologia *blockchain* se conturează drept o soluţie pentru una dintre cele mai mari şi acute probleme ale publicităţii comerciale *online*, şi anume frauda în executarea contractuală. Din cercetarea realizată, reiese că ar avea chiar potenţialul de a o elimina complet, ceea ce ar conduce la sume mai mari alocate unui marketing de calitate (calitatea fiind dată de executarea conformă fără de care plata nu poate fi realizată).

La momentul actual, industria publicităţii *online* are un potenţial prejudiciator pentru toţi actorii implicaţi, în parte şi din cauza intervenţiei factorului uman.

95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE), OJ L 119, 4.5.2016, pp. 1–88.

[140] A. Wallace, *Protection of Personal Data in Blockchain Technology. An investigation on the compatibility of the General Data Protection Regulation and the public blockchain*, Master's Thesis, 2018, [Online] la https://www.diva-portal.org/smash/get/diva2:1298747/FULLTEXT01.pdf, accesat 30.11.2021, p. 48.

[141] *Idem*, p. 47.

[142] Pentru mai multe detalii, a se vedea, [Online] https://www.forbes.com/sites/thomasbrewster/2019/01/23/ether-scammers-made-36-million-in-2018double-their-2017-winnings/, accesat 30.11.2021.

[143] SaTT Token, *Smart Advertising Transaction Token (SaTT),* White Paper, p. 32

[144] ING Bank, European Central Bank, *Cryptocurrencies and tokens*, September 2018, …, p. 8.

Astfel, adiacent subminării fraudei, tehnologia *blockchain* contribuie, prin automatizare, atât la creşterea încrederii părţilor contractuale în executarea contractului, cât şi la creşterea încrederii consumatorilor. În acest mod, se va ajunge la o creştere şi mai susţinută a industriei publicităţii *online*, atingând o dimensiune chiar astronomică[145], care ar leza mai puţin interesele profesioniştilor şi ale consumatorilor. Existenţa neexecutării, precum şi a litigiilor, nu îşi vor mai avea locul în *smart contracts*.

Tehnologia *blockchain* va aduce cu sine o schimbare a ecosistemului publicitar în principal prin modificarea numărului participanţilor implicaţi şi prin naşterea unor noi modalităţi de stabilire şi plată a preţului. Apariţia unor viitoare reglementări în domeniu vor putea să diminueze dezavantajele pe care utilizarea tehnologiei *blockchain* în publicitatea comercială *online* le prezintă momentan.

Referinţe

Atzori M., Sistemi I., *Blockchain technology and decentralized governance: Is the state still necessary?*, în Journal of Governance and Regulation 6(1), March 2017, DOI: https://doi.org/10.22495/jgr_v6_i1_p5

Bleier A., Eisenbeiss M., *Personalized Online Advertising Effectiveness: The Interplay of What, When, and Where*, July 2015, Marketing Science, 2015, DOI: https://doi.org/10.1287/mksc.2015.0930

Corrales M., Fenwick M., Haapio H., *Digital Technologies, Legal Design and the Future of the Legal Profession* în M. Corrales, M. Fenwick, H. Haapio (eds.), *Legal tech,* Smart contracts *and Blockchain,* Springer Nature Singapore Pte Ltd., 2019

Daswani N., Mysen C., Rao V., Weis S., Gharachorloo K., Ghosemajumder S., the Google Ad Traffic Quality Team, *Online Advertising Fraud*, 2007

Išoraitė M., *Raising Brand Awarenees Through The Internet Marketing Tools*, în Independent Journal of Management & Production (IJM&P), v. 7, n. 2, April - June 2016, DOI: https://doi.org/10.14807/ijmp.v7i2.39

Jain A., Khan S., *Optimizing Cost per Click for Digital Advertising Campaigns*, în Lattice, Volume 2, Issue 2, 2021

Jaina D., Dashb M. K., Kumarc A., Luthra S., *How is Blockchain used in marketing: A review and research agenda*, în International Journal of Information Management Data Insights, DOI: https://doi.org/10.1016/j.jjimei.2021.100044

Kadekova Z., Holienčinová M., *Influencer marketing as a modern phenomenon creating a new frontier of virtual opportunities* în Communication Today, no. 9, 2018

Koen P., Reibstein D., *Challenges in Measuring Return on Marketing Investment: Combining Research and Practice Perspectives,* Review of Marketing Research vol. 6. Emerald Group Publishing Limited, Bingley, 2009, DOI: https://doi.org/10.1108/S1548-6435(2009)0000006009

Lashkari B., Musilek P., *A Comprehensive Review of Blockchain Consensus Mechanisms*, în IEEE Access PP(99): 1-1, DOI: https://doi.org/10.1109/ACCESS.2021.3065880

Mammadzada K., Milani F., Iqbal M., García-Bañuelos L., *Blockchain Oracles: A Framework for Blockchain-Based Applications*, în Business Process Management: Blockchain and Robotic Process Automation Forum, BPM 2020 Blockchain and RPA Forum, Seville, Spain, September 13–18, 2020, Proceedings (pp.19-34), DOI: https://doi.org/10.1007/978-3-030-58779-6_2

[145] PwC, *Is blockchain the answer to digital advertising's trust gap?*, ..., p. 6.

Muthukrishnan S., *Ad Exchanges: Research Issues*, în Leonardi S. (eds), *Internet and Network Economics*, WINE, Lecture Notes in Computer Science, vol 5929. Springer, Berlin, Heidelberg, 2009, DOI: https://doi.org/10.1007/978-3-642-10841-9_1

Nazerzadeh H., Saberi A., Vohra R., *Dynamic Cost-Per-Action Mechanisms and Applications to Online Advertising*, în Internet Monetization - *Online* Advertising, April 21-25, Beijing, China, 2008

Pooranian Z., Conti M., Haddadi H., Tafazolli R., *Online Advertising Security: Issues, Taxonomy, and Future Directions*, în IEEE Communications Surveys & Tutorials, vol. XX, vo. NN, XX, 2020

Rawat D. B., Vijay Chaudhary V., Doku R. , Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems, în Journal of Cybersecurity and Privacy no. 1(1), 2021

Seang S., Torre D., *Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies*, GREDEG Working Papers 2019-24, Groupe de REcherche en Droit, Economie, Gestion (GREDEG CNRS), Université Côte d'Azur, France

Silberholz J., Ross S. M., Wu Di (A.), *Measuring Utility and Speculation in Blockchain Tokens*, September 1, 2021, DOI: http://dx.doi.org/10.2139/ssrn.3915269

Tuleaşcă L., *Dreptul comerţului internaţional. Tranzacţii comerciale internaţionale*, Editura Universul Juridic, Bucureşti, 2017

Ungureanu C. T., *Drept international privat european in raporturi de comert international*, Editura Hamangiu, Bucureşti, 2021, p. 37

Ungureanu C. T., Toader A. I., *Drept civil. Partea generală. Persoanele*, Editura Hamangiu, Bucureşti, 2019

Ungureanu C. T., *Dreptul comerţului internaţional*, Editura Hamangiu, Bucureşti, 2018

Wallace A., *Protection of Personal Data in Blockchain Technology. An investigation on the compatibility of the General Data Protection Regulation and the public blockchain*, Master's Thesis, 2018

Zamfir M., Manea M., Ionescu L., *Return On Investment – Indicator for Measuring the Profitability of Invested Capital*, în Valahian Journal of Economic Sciences vol. 7(2), 2016, DOI: https://doi.org/10.1515/vjes-2016-0010

Zeropark Blog, What Is the Difference Between CPM, CPC, CPL, CPA and Other Performance Marketing Pricing Models?, 28th of May, 2021

Zhang R., Xue R., Liu L., *Security and Privacy on Blockchain* în ACM Comput. Surv. 1, 1, Article 1, January, DOI: https://doi.org/10.1145/3316481

European Parliament, *Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice*, Study Requested by the IMCO committee, June 2021, DOI: https://doi.org/10.2861/80 | QA-02-21-683-EN-N

IAB Romania, 2Performant, Consiliul Român pentru Publicitate, *Cod de bune practici în influencer marketing*, România, 2020, [Online]

Inland Revenue Authority of Singapore, *Digital Payment Tokens*, [Online]

Innovation Lab (IDB Lab) of the Inter-American Development Bank, *Cross-Border Payments with Blockchain*, 2021, [Online]

Content Strategy Studio, *Brand Engagement in the Participation Age*, Whitepaper, February 2014 , [Online]

ING Bank, European Central Bank, *Cryptocurrencies and tokens*, September 2018, [Online]

Invao, *Token Classes Explained: Coin vs. Utility Token vs. Security Token*, [Online]

Kenton W., *Cost Per Thousand (CPM)*, Investopedia, October 29, 2020, [Online]

MoPub Inc., *Understanding ad networks*, 2017, [Online]

Open X, *Ad networks vs ad exchanges: how they stack up*, 2010, [Online]
PwC, *Is blockchain the answer to digital advertising's trust gap?*, 2019, [Online]
PwC, *Macrotrends. Global revenue – growth by segments*, [Online]
TATA Consulting Services, *Digital Advertising, Blockchain(ed)*, White Paper, 2017, [Online]
Token Alliance, Chamber of Digital Commerce, *Understanding Digital Tokens. Legal Landscapes Governing Digital Tokens in the European Union*, May 2021, [Online]

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-10

Utilizarea *blockchain* în soluţionarea litigiilor

Blockchain Dispute Resolution

Tudor-Matei Rusu[1]

Rezumat: Nu prezintă o noutate faptul că persoanele, din dorinţa de a soluţiona cât mai rapid un litigiu, apelează cât mai des la mijloace alternative. Această situaţie este întâlnită, preponderent, în cazurile în care obiectul litigiului este unul relativ redus. Nici utilizarea platformelor online de soluţionare a litigiilor nu mai prezintă o noutate, acestea devenind din ce în ce mai folosite în ultima perioadă. Un aspect de noutate este reprezentat, însă, de utilizarea tehnologiei *blockchain* în soluţionarea litigiilor. Prin utilizarea acestei tehnologii, platformele online structurează întreaga procedură dar îi şi remunerează pe utilizatorii ce au rolul de a soluţiona litigiile. Totodată, tehnologia *blockchain* poate fi utilizată concomitent cu anumiţi algoritmi în aşa fel încât litigiile să fie soluţionate fără intervenţia factorului uman.

Cuvinte-cheie: *blockchain*; mijloace alternative de soluţionare a litigiilor; mijloace online de soluţionare a litigiilor; platforme de intermediere; *Kleros*

Abstract: The alternative dispute resolution methods *(ADR)* are not something new, neither the online dispute resolution platforms *(ODR).* In the last period of time more and more online platforms started to use blockchain to settle disputes. The blockchain technology is used by the platforms to set up arbitration, organize dispute adjudication and reward the arbitrators. Also, it can be used in a way which allows the disputing parties interact with each other through the platform, while the latter acts like a mediator, using algorithms that facilitate the interaction between the parties.

Keywords: blockchain; alternative dispute resolution methods (ADR); online dispute resolution methods (ODR); online platforms; Kleros

Precizări introductive

Mijloacele alternative de soluţionare a litigiilor nu mai prezintă o noutate. Astfel, de-a lungul timpului, în special din cauza supraîncărcării instanţelor statale, a existat o încercare de a încuraja metode precum medierea, concilierea, *dispute board* sau *minitrial*[2].

[1] Doctorand, Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iași, e-mail: tmrusu@gmail.com.

[2] C.T. Ungureanu, *Dreptul comerțului internațional*, Editura Hamangiu, București, 2018, p. 312.

Datorită dezvoltării tehnologice, dar şi a expansiunii Internetului, unele dintre mijloacele alternative de soluţionare a litigiilor au fost transpuse în mediul online, apărând conceptul de *Online Dispute Resolution (ODR).* Acesta reprezintă o nouă modalitate alternativă de soluţionare a litigiilor ce presupune folosirea unei platforme online. În cadrul *ODR*, procesul de luare a unei decizii este facilitat de capacitatea de stocare şi de procesare a datelor de către calculatoare, dar şi de utilizarea Internetului[3].

Participanţii beneficiază şi de o serie de garanţii specifice Internetului. Astfel, în cadrul procedurii de soluţionare alternativă a unui litigiu în mediul online pot fi instituite măsuri de siguranţă precum autentificarea utilizatorilor în doi factori[4] şi criptarea informaţiilor transmise de către aceştia[5].

Nu orice utilizare a tehnologiei cu scopul de a facilita soluţionarea unui litigiu presupune, în mod automat, şi folosirea unei metode alternative. Conceptul de *ODR* presupune mai mult decât stocarea datelor în format electronic sau audierea unui martor prin videoconferinţă. Aceste două exemple reprezintă doar modalităţi în care tehnologia este folosită pentru a facilita bunul mers al justiţiei. Totodată, nici posibilitatea pe care o au unii consumatori[6] de a trimite o plângere în format electronic societăţii de la care au achiziţionat un bun sau un serviciu nu presupune existenţa unui mijloc alternativ de soluţionare a litigiilor în cazurile în care acea plângere nu este dublată şi de existenţa unui sistem concret ce are rolul de a preîntâmpina o posibilă judecată. În această situaţie, plângerile consumatorilor

[3] R.D. Stângaciu, *Limite ale implicării tehnologiei în soluționarea prin mijloace alternative a litigiilor Online Dispute Resolution prin prisma raporturilor de comerț internațional*, în Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" Iaşi, Tomul LXV, Ştiinţe Juridice, 2019, Supliment, p. 161, [Online] la http://pub.law.uaic.ro/files/articole/ 2019/vols/11. stangaciu.pdf, accesat 10.11.2021; A. Gudkov, *Crowd Arbitration: Blockchain Dispute Resolution*, în Legal Issues in the Digital Age, Nr. 3, 2020, DOI: https://doi.org/ 10.17323/2713-2749.2020.3.59.77, accesat 10.11.2021, p. 60.

[4] Prin *autentificarea în doi factori*, utilizatorul trebuie să ofere două coduri de acces atunci când accesează respectiva platformă, iar acest lucru oferă o protecţie suplimentară atât pentru propria persoană, cât şi pentru platforma accesată. A se vedea, L. Rosencrance, P. Loshin, M. Cobb, *Two-factor authentication (2FA)*, [Online] la https://www.techtarget. com/searchsecurity/definition/two-factor-authentication, accesat 10.11.2021.

[5] W. Gonzales, N. Masumy, *Online Dispute Resolution Platforms: Cybersecurity Champions in the COVID-19 Era? Time for Arbitral Institutions to Embrace ODRs*, în Kluwer Arbitration Blog, [Online] la http://arbitrationblog.kluwerarbitration.com/2020/09/ 25/online-dispute-resolution-platforms-cybersecurity-champions-in-the-covid-19-era-time-for-arbitral-institutions-to-embrace-odrs/, accesat 10.11.2021.

[6] Noţiunea de consumator poate fi definită, conform art. 2 pct. 2 din O.G. nr. 21/1992 privind protecţia consumatorilor, republicată în M. Of. al României, Partea I, nr. 208 din 28 martie 2007, ca fiind „*orice persoană fizică sau grup de persoane fizice constituite în asociații, care acționează în scopuri din afara activității comerciale, industriale sau de producție, artizanale ori liberale*".

se încadrează în sfera recenziilor pe care le cere societatea de la care au achiziţionat respectivul bun sau serviciu[7].

1. Platformele Online Dispute Resolution (ODR Platforms)

Odată cu apariţia conceptului de *ODR* a apărut şi noţiunea de *platformă ODR*, deoarece modalitatea de soluţionare alternativă a litigiilor în mediul online este indisolubil legată de existenţa unei platforme.

O platformă *ODR* este o pagină *web* ce oferă utilizatorilor săi posibilitatea de a se înregistra şi de a o utiliza cu scopul de a le fi soluţionat un posibil litigiu izvorât dintr-un contract încheiat în mediul online. Deşi modul de funcţionare diferă de la o platformă la alta, de regulă, utilizatorii accesează acest mod de soluţionare alternativă a litigiilor prin completarea unui formular tipizat în cadrul platformei şi, totodată, ei trebuie să ataşeze documentele prin care îşi justifică pretenţiile[8].

În contextul creşterii numărului de procese dintre participanţii la activităţile de comerţ online, a devenit evident că era necesară o modalitate eficientă şi rapidă de soluţionare a acestor categorii de litigii. Una dintre primele platforme de intermediere ce a oferit utilizatorilor săi şi o secţiune dedicată soluţionării amiabile a litigiilor a fost *eBay*[9].

Serviciile oferite de platformele online de soluţionare a litigiilor sunt adaptate la caracteristicile Internetului, oferind utilizatorilor, ce se află la distanţă unul faţă de altul, mijloacele necesare pentru a-şi comunica cererile şi dovezile. Totodată, platformele *ODR* nu aduc o schimbare semnificativă faţă de mijloacele alternative de soluţionare a litigiilor, ele doar transpun aceste mijloace în mediul online[10].

Nu doar platformele de intermediere au urmărit dezvoltarea unor centre online de soluţionare alternativă a litigiilor, inclusiv autorităţile publice au considerat necesară existenţa unor astfel de metode. Platformele *ODR*, în funcţie de entitatea ce le pune la dispoziţie, pot fi clasificate în platforme private şi publice[11].

---

[7] A.H. Raymond, S.J. Shackelford, *Technology, Ethics, and Access to Justice: Should an Algorithm be Deciding Your Case?*, în Michigan Journal of International Law, Vol. 35, Nr. 3, 2014, p. 500, [Online] la http://repository.law.umich.edu/mjil/vol35/iss3/1, accesat 10.11.2021.

[8] J. Barnett, P. Treleaven, *Algorithmic Dispute Resolution – The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies*, în The Computer Journal, Section C: Computational Intelligence, Machine Learning and Data Analytics, Vol. 61, Nr. 3, 2018, DOI: https://doi.org/10.1093/comjnl/bxx103, accesat 10.11.2021, p. 403.

[9] M. Dylag, H. Smith, *From cryptocurrencies to cryptocourts: blockchain and the financialization of dispute resolution platforms*, în Information, Communication & Society, p. 3, [Online] la https://www.tandfonline.com/doi/full/10.1080/13691 18X.2021.1942958, accesat 13.11.2021.

[10] *Idem*, p. 4.

[11] A.H. Raymond, S.J. Shackelford, *op. cit.*, p. 501.

Cele private, care sunt puse la dispoziţie de către o întreprindere[12], pot fi subclasificate în funcţie de serviciile oferite utilizatorilor. O primă categorie este reprezentată de platformele *self-contained*, care nu există de sine stătător, ci fac parte dintr-o comunitate deja existentă şi au rolul de a soluţiona litigii în cadrul acesteia. Astfel, cel mai bun exemplu este reprezentat de centrul de soluţionare a litigiilor din cadrul platformei *eBay*[13]. Rolul acestui centru este de a facilita comunicarea dintre cumpărător şi vânzător în cazul în care există probleme cu privire la contractul intermediat de platformă. În momentul în care una dintre părţile contractului este nemulţumită de modul în care cealaltă a executat obligaţiile, poate să apeleze la acest centru de soluţionare a litigiilor. Odată începută procedura, părţile au la dispoziţie un termen de trei zile în care pot ajunge la un consens, iar din momentul în care este împlinit termenul şi acestea nu au ajuns la un consens, oricare dintre ele poate apela la un reprezentat al platformei pentru soluţionare[14].

Nu trebuie făcută confuzia între funcţiile de soluţionare alternativă a litigiilor din cadrul platformelor de intermediere cu posibilitatea pe care o au utilizatorii de a posta recenzii negative la adresa vânzătorilor. Prin simplul fapt că oferă o recenzie, cumpărătorul nu urmăreşte şi soluţionarea pe cale amiabilă a problemei pe care o are referitoare la modul în care vânzătorul a executat obligaţiile asumate prin contract.

Un avantaj al acestui tip de platforme este acela că, în cadrul sistemului deja existent, pot fi luate şi alte măsuri în afară de soluţionarea alternativă a litigiilor. Astfel, platforma poate suspenda contul unui vânzător dacă împotriva acestuia există un anumit număr de plângeri în cadrul centrului de soluţionare a litigiilor. Totodată, inclusiv mecanismul de plată este structurat în aşa fel încât plata are loc prin intermediul mijloacelor puse la dispoziţie de platformă şi, dacă se constată că vânzătorul nu şi-a respectat obligaţiile, platforma poate dispune, în baza acordului încheiat cu utilizatorul-vânzător, ca suma plătită să fie returnată de către acesta din urmă în cazul în care se ajunge la o soluţie prin intermediul centrului de soluţionare a litigiilor[15].

O a doua categorie este reprezentată de platformele *full service*. Acestea au o existenţă de sine stătătoare şi, astfel, nu se mai limitează la o anumită comunitate deja existentă şi oferă acces oricărei persoane la serviciile lor. Spre deosebire de cele *self-contained*, acestea nu mai oferă şi alt serviciu utilizatorilor, soluţionarea online a litigiilor fiind singurul lor obiect de activitate. Un bun exemplu este platforma *Modria*[16]. Atunci când un utilizator apelează la serviciile oferite de

[12] Este folosită noțiunea de întreprindere, deoarece, conform art. 3 alin. (2) din Codul civil român (republicat în M. Of. al României, Partea I, nr. 505 din 15 iulie 2011), „*sunt considerați profesioniști toți cei care exploatează o întreprindere.*”.

[13] A se vedea, *eBay Resolution Center*, [Online] la https://resolutioncenter.ebay.com/, accesat 13.11.2021.

[14] A.H. Raymond, S.J. Shackelford, *op. cit.*, p. 501.

[15] *Idem*, p. 502.

[16] [Online] la https://www.tylertech.com/products/Modria, accesat 15.11.2021.

aceasta, trebuie să ofere toate detaliile şi dovezile necesare, iar, platforma, în baza unor algoritmi, sugerează o soluţie părţilor. Totodată, acestea pot să şi comunice prin intermediul platformei şi, dacă nu ajung la un consens în baza soluţiei generate automat, ele sunt îndemnate să apeleze la procedura medierii, procedură ce are loc, dacă părţile doresc, tot în cadrul platformei[17].

De-a lungul timpului, platformele *ODR* s-au confruntat cu o problemă legată de costurile proprii. Astfel, costurile ocazionate de acestea erau vădit disproporţionate comparativ cu valoarea obiectelor litigiilor ce erau soluţionare prin intermediul lor[18]. Dar, evoluţia tehnologică, a făcut posibilă eliminarea celui mai costisitor element, factorul uman. În acest sens, platformele *ODR* au început, treptat, să îşi automatizeze tot mai mult procedurile, apelând la algoritmi[19].

În prezent, în cadrul platformelor *Modria*, *SmartSettle*[20] şi *CyberSettle*[21] atât procedurile de negociere, cât şi cele de mediere se desfăşoară fără intervenţia factorului uman. În cazul negocierii, sunt oferite mijloace de comunicare părţilor, iar în cazul medierii, sunt utilizaţi algoritmi ce găsesc o soluţie ce este, mai apoi, comunicată părţilor, urmând ca acestea să decidă dacă sunt sau nu de acord cu soluţia identificată[22].

2. Blockchain Dispute Resolution (BDR)

Asemenea *ODR* şi *BDR* reprezintă o metodă de soluţionare alternativă a litigiilor ce este indisolubil legată de existenţa unei platforme online, doar că, spre deosebire de mijloacele discutate anterior, *BDR* foloseşte tehnologia *blockchain* în procesul de soluţionare alternativă a litigiilor.

2.1. Definirea termenilor de blockchain şi blockchain dispute resolution

Tehnologia *blockchain* reprezintă o modalitate de stocare a datelor într-un sistem descentralizat, ce face, datorită caracteristicilor sale, foarte dificilă sau chiar imposibilă modificarea datelor prin accesarea neautorizată a sistemului. Practic, *blockchain*-ul presupune o bază de date descentralizată, alcătuită dintr-o multitudine de calculatoare, interconectate ce au rolul de a stoca date simultan, în aşa fel încât fiecare dată stocată să fie găsită în fiecare calculator din sistem[23].

Având o structură descentralizată şi interconectată, *blockchain*-ul prezintă mult mai multă siguranţă faţă de o bază de date obişnuită, aceasta bazându-se pe o singură sursă de stocare a datelor. Totodată, de fiecare dată când se doreşte

[17] A.H. Raymond, S.J. Shackelford, *op. cit.*, p. 503; J. Barnett, P. Treleaven, *op. cit.*, p. 404.

[18] Este de natura soluționării alternative a litigiilor ca la aceste metode să se apeleze, în special, în cazul litigiilor de o importanţă mai redusă.

[19] A.H. Raymond, S.J. Shackelford, *op. cit.*, p. 514.

[20] [Online] la https://www.smartsettle.com/, accesat 15.11.2021.

[21] [Online] la http://www.cybersettle.com/, accesat 15.11.2021.

[22] J. Barnett, P. Treleaven, *op. cit.*, p. 404.

[23] A se vedea, *What is blockchain?*, [Online] la https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain, accesat 15.11.2021.

înregistrarea unei noi informaţii în sistem, este necesar acordul tuturor calculatoarelor interconectate, iar acest lucru sporeşte gradul de transparenţă[24].

Tehnologia *blockchain* a apărut ca o reacţie contra autorităţii statale şi a fost şi folosită cu scopul de a mai reduce din implicarea statului în anumite domenii în care se considera că acesta deţine o putere absolută[25]. În acelaşi timp, progresul tehnologic şi expansiunea Internetului au stat întotdeauna la baza soluţionării litigiilor în mediul online, iar tehnologia *blockchain* nu face excepţie, putând reprezenta o nouă soluţie pentru mijloacele alternative de soluţionare a litigiilor.

Termenul *blockchain dispute resolution* este folosit pentru a descrie o procedură descentralizată de soluţionare alternativă a litigiilor, desfăşurată în mediul online, ce utilizează tehnologia *blockchain* pentru a organiza procesul de soluţionare şi de executare a hotărârii luate, dar şi pentru a-i remunera pe cei care iau hotărârea[26].

Alternativ, pentru a descrie acelaşi mod de soluţionare a litigiilor, sunt utilizate noţiunile de *crypto instanţe* şi *crowdsourced dispute resolution*[27]. Ultimul dintre termeni este utilizat pentru a face referire la persoanele care soluţionează litigiile. În cadrul acestei metode, persoanele ce urmează să soluţioneze un litigiu nu trebuie să aibă o calitate anume, oricine doreşte poate să participe la o astfel de procedură. Mai mult decât atât, persoanele care soluţionează litigiul nu doar că nu trebuie să îndeplinească nicio cerinţă, dar sunt şi necunoscute părţilor. De aici şi reiese termenul de *crowdsourced dispute resolution*, deoarece rolul decizional este transferat unui număr foarte mare de persoane, a căror provenienţă este necunoscută şi cărora nu li se cere nicio cunoştinţă juridică[28].

Din acest punct de vedere, soluţionarea litigiilor prin utilizarea tehnologiei *blockchain* se deosebeşte nu doar de situaţia în care se apelează la instanţele statale sau arbitrale, ci şi de celelalte metode alternative de soluţionare a litigiilor, deoarece, inclusiv în cadrul acestora, persoana ce soluţionează litigiul este cunoscută de părţi, dacă nu este chiar aleasă de către acestea.

A existat, totodată, şi o iniţiativă de a utiliza tehnologia *blockchain* în cadrul procedurilor judiciare desfăşurate în faţa instanţelor statale. Astfel, în Marea Britanie, prin intermediul unui program pilot ce a debutat în anul 2018 s-a analizat dacă activitatea de stocare a documentelor poate fi realizată prin intermediul unei baze de date *blockchain*[29].

[24] J. Barnett, P. Treleaven, *op. cit.*, p. 403.

[25] V. Gupta, *A Brief History of Blockchain*, în Harvard Business Review, [Online] la https://hbr.org/2017/02/a-brief-history-of-blockchain, accesat 15.11.2021.

[26] A. Gudkov, *op. cit.*, p. 60.

[27] *Idem*, p. 62.

[28] A. Gudkov, *op. cit.*, p. 62.

[29] M. Dylag, H. Smith, *op. cit.*, p. 5; S. Seth, *UK Courts Start Pilot Blockchain Evidence System*, [Online] la https://www.investopedia.com/news/uk-courts-start-pilot-blockchain-evidence-system/, accesat 16.11.2021.

2.2. Clasificarea platformelor *BDR*

Asemenea platformelor *ODR* şi platformele ce utilizează tehnologia *blockchain* într-un proces de soluţionare alternativă a litigiilor pot fi clasificate în funcţie de principalul serviciu pus la dispoziţia utilizatorilor. Astfel, această activitate poate fi singura pe care o desfăşoară platforma sau poate să reprezinte un serviciu adiţional celui principal, pus la dispoziţia propriilor utilizatori[30].

În cazul în care activitatea de soluţionare a litigiilor reprezintă singurul serviciu oferit de platformă, aceasta nu se bazează pe o comunitate deja existentă. Astfel, oricine poate să apeleze la respectivul serviciu pus la dispoziţie pentru a-i fi soluţionat un litigiu izvorât dintr-un contract încheiat în mediul online. Este posibil, cu toate acestea, să fie introduse filtre cu privire la litigiile ce pot fi soluţionate. Platformele *Kleros*[31], *Rhubarb*[32] şi *Aragon*[33] sunt unele dintre cele ce oferă acces la serviciile lor de soluţionare alternativă a litigiilor tuturor persoanelor doritoare şi a căror litigii respectă anumite condiţii ce diferă de la o platformă la alta[34].

Deşi acestea nu se bazează pe o comunitate deja existentă deoarece nu oferă decât serviciul de soluţionare a litigiilor, în mod automat, ele se adresează unei sfere bine stabilite de persoane, unui ecosistem identificabil. Astfel, este normal ca, prin utilizarea *blockchain*-ului să se urmărească atragerea persoanelor ce sunt familiarizate cu acest fenomen şi care intră în contact cu respectiva tehnologie. Spre exemplu, *Kleros* oferă posibilitatea de a apela la serviciile sale numai persoanelor fizice sau întreprinderilor ce au încheiat un *smart contract* ce respectă condiţiile prevăzute în mod expres în cadrul platformei[35].

Există posibilitatea ca unele platforme să ofere, pe lângă serviciile principale puse la dispoziţia utilizatorilor, şi o modalitate de soluţionare alternativă a litigiilor dintre aceştia, iar această metodă să fie pusă în aplicare prin intermediul tehnologiei *blockchain*. În acest caz, datorită principalului serviciu pus la dispoziţie, există o comunitate bine închegată, iar, în cadrul acesteia, pot apărea probleme referitoare la modul în care părţile îşi execută obligaţiile contractuale. În astfel de situaţii, activitatea de soluţionare alternativă a litigiilor presupune un serviciu adiţional pus la dispoziţia utilizatorilor[36].

Întreprinderea din China, *Baidu*[37], ce oferă utilizatorilor săi un motor de căutare, dar şi alte servicii ce ţin de domeniul Internetului, a dezvoltat, în colaborare cu *Comisia Arbitrală din Qingdao*, un sistem de soluţionare a litigiilor în mediul online, sistem ce utilizează tehnologia de tip *blockchain* pentru a stoca şi transmite

[30] A. Gudkov, *op. cit.*, p. 62.
[31] [Online] la https://court.kleros.io/, accesat 16.11.2021.
[32] [Online] la https://www.rhucoin.com/, accesat 16.11.2021.
[33] [Online] la https://anj.aragon.org/#/dashboard, accesat 16.11.2021.
[34] A. Gudkov, *op. cit.*, p. 62.
[35] [Online] la https://github.com/kleros, accesat 16.11.2021.
[36] A. Gudkov, *op. cit.*, p. 63.
[37] [Online] la http://www.baidu.com/, accesat 17.11.2021.

informaţii[38]. Şi platforma de intermediere *Alibaba*[39] a dezvoltat un serviciu adiţional, bazat pe tehnologia *blockchain*, ce are rolul de a le permite propriilor utilizatori să îşi rezolve litigiile apărute în legătură cu contractele încheiate în cadrul platformei.

2.3. Avantajele şi dezavantajele *BDR*

O metodă alternativă de soluţionare a litigiilor, ce utilizează *blockchain*-ul şi se adresează, cu precădere, litigiilor izvorâte din contracte încheiate în mediul online, este de aşteptat să presupună atât avantaje, cât şi dezavantaje pentru cei ce doresc să apeleze la aceasta.

Din moment ce întreaga procedură presupune o soluţionare descentralizată a litigiilor, majoritatea avantajelor şi a dezavantajelor sunt generate de faptul că, spre deosebire de situaţia instanţelor statale sau arbitrale, soluţia este luată fie în baza unor algoritmi, fie de către persoane necunoscute.

2.3.1. Avantajele BDR

Un prim avantaj este reprezentat de faptul că, datorită modului în care este gândită procedura, este imposibilă identificarea utilizatorilor ce au rolul de a soluţiona litigiile. Astfel, nu este niciodată făcută publică identitatea acestora, în cadrul platformei fiind cunoscută doar *crypto adresa*[40], pseudonimul sau adresa de *email*. Practic, litigiul este soluţionat de către mai mulţi utilizatori anonimi, iar nici aceştia nu pot să cunoască persoana celuilalt. Astfel, decizia este luată de către persoane ce nu se cunosc, nu au încredere una în cealaltă şi nici nu cunosc persoanele al cărui litigiu îl tranşează, acest lucru facând ca accentul să fie pus pe problemă în sine şi nu pe părţi[41].

Deşi persoanele sunt necunoscute, anonime, istoricul acestora referitor la litigiile soluţionate anterior poate fi verificat prin intermediul *crypto adresei*. Iar din moment ce toate datele referitoare la istoricul persoanei în cadrul *ecosistemului* sunt transparente şi pot fi verificate de către participanţii la procedură, se reduce din riscul creat de faptul că identitatea sa nu este cunoscută de aceştia[42].

Un al doilea avantaj este reprezentat de modul în care are loc punerea în aplicare a deciziei luate. Spre deosebire de situaţia în care litigiul este soluţionat de către instanţele statale sau arbitrale, în cadrul *BDR* nu mai este necesară nicio acţiune din partea părţii ce nu a avut câştig de cauză. Totodată, nu mai este

[38] A. Gudkov, *op. cit.*, p. 63; M. Wood, *Baidu launches judicial arbitration blockchain*, [Online] la https://www.ledgerinsights.com/baidu-judicial-arbitration-blockchain/, accesat 17.11.2021.

[39] [Online] la https://www.alibaba.com/?spm=a27aq.22871746.scGlobalHomeHeader.8.13ae3bdbBUwVJ1, accesat 17.11.2021.

[40] *Crypto adresa* presupune un şir de caractere (atât litere, cât şi cifre) ce are rolul de a identifica titularul unui cuantum de *cryptomonedă*. Este imposibil ca două persoane să aibă aceeaşi *crypto adresă*. A se vedea, *What Is My Bitcoin Address and How Does It Work?*, [Online] la https://unblock.net/bitcoin-address-work/, accesat 18.11.2021.

[41] A. Gudkov, *op. cit.*, p. 63.

[42] *Ibidem*.

necesară nici apelarea la forţa de constrângere a statului pentru a o obliga pe una dintre părţi să execute silit hotărârea, în cazul în care aceasta nu a executat hotărârea de bunăvoie. În această situaţie, soluţia luată este pusă în executare în mod automat de către platformă. Executarea are loc imediat prin intermediul unui *smart contract*[43] încheiat între părţi la începutul procedurii[44].

Alternativ termenului de *blockchain dispute resolution*, pentru a descrie aceeaşi metodă alternativă de soluţionare a litigiilor, este folosită şi noţiunea de *crowdsourced dispute resolution*, aşa cum deja am menţionat. Astfel, se pune accentul pe numărul mare şi, oarecum, aleatoriu al celor ce pot soluţiona litigii prin intermediul unei astfel de proceduri. Unii autori chiar aseamănă această metodă cu modul în care curţile cu juraţi soluţionează un litigiu[45].

Teoretic, cu cât numărul celor ce soluţionează un litigiu este mai mare, şansele ca aceştia să ajungă la o concluzie greşită sunt din ce în ce mai mici. Totodată, deciziile sunt luate, de regulă, fără o colaborare între cei ce tranşează problema, iar acest lucru scade, la rândul său, riscul ca utilizatorii platformei să ajungă la o decizie greşită, deoarece ei nu se pot influenţa reciproc. Din aceste motive este utilizat şi termenul de *wisdom of the crowd* pentru a descrie modul în care sunt luate hotărârile în cadrul unei astfel de metode de soluţionare a litigiilor[46].

Metoda devine ineficientă în cazul în care numărul celor ce soluţionează litigiile este redus. Dar, din moment ce fiecare caz aparte diferă şi procedurile stabilite de fiecare platformă diferă la rândul lor, este dificil de stabilit ce presupune un număr redus de persoane raportat la fiecare caz în parte. Spre exemplu, în cadrul centrului de soluţionare alternativă a litigiilor pus la dispoziţie de platforma *Alibaba*, litigiile sunt soluţionate în cadrul unor paneluri la care iau parte 31 de persoane. Totodată, numărul de cauze pe care le poate soluţiona un utilizator într-o zi este limitat la 20[47]. În cadrul platformei *Kleros*, litigiile sunt soluţionate de către un număr de trei sau de cinci persoane, în funcţie de obiectul litigiului[48].

Diferenţa dintre cele două exemple anterioare este dată de faptul că, în cadrul *Kleros*, litigiile tind să prezinte un grad mai mare de dificultate, soluţionarea acestora luând şi mai mult timp. Spre exemplu, jumătate dintre cei ce folosesc platforma consideră că pot soluţiona zilnic între două şi cinci cauze. În acelaşi timp, utilizatorii *Kleros* tind să fie şi mai bine pregătiţi comparativ cu utilizatorii altor platforme asemănătoare. Conform unui studiu, 86% dintre utilizatori sunt capabili

[43] Termenul de *smart contract* presupune, de fapt, un program redactat în limbaj informativ ce este înregistrat într-o bază de date de tip *blockchain*. A se vedea, *What are smart contracts on blockchain?*, [Online] la https://www.ibm.com/topics/smart-contracts, accesat 18.11.2021.

[44] A. Gudkov, *op. cit.*, p. 64.

[45] *Ibidem.*

[46] A. Gudkov, *op. cit.*, p. 65.

[47] D. Dimov, *Crowdsourced online dispute resolution*, în Leiden University Center for Law and Digital Technologies, [Online] la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3003815, accesat 20.11.2021.

[48] A. Gudkov, *op. cit.*, p. 67.

să rezolve exerciţii de logică dificile şi complexe, iar peste 80% dintre aceştia sunt familiarizaţi cu termenii juridici ce pot fi întâlniţi în timpul soluţionării litigiilor[49].

Un alt avantaj este reprezentat de faptul că oricine poate să apeleze la această modalitate de soluţionare a litigiilor. Platformele nu limitează utilizatorii la o anumită zonă geografică şi, totodată, nu doar cei ce folosesc tehnologia *blockchain* pot să apeleze la serviciile oferite de acestea. Practic, oricine acceptă condiţiile platformei poate să ceară să îi fie soluţionată problema astfel.

Un ultim avantaj este cel legat de eficienţă. Astfel, *BDR* reprezintă o soluţie în special pentru cazurile în care obiectul litigiului are o valoare relativ redusă. Durata procedurilor desfăşurate în faţa instanţelor statale sau în faţa instanţelor arbitrale tinde să fie una destul de mare şi în cazul în care litigiul are o importanţă relativ redusă nu este utilă aşteptarea unui timp îndelungat pentru ca problema să fie soluţionată. Dar, în cazul unui litigiu important, a cărui obiect are o valoare semnificativă, *BDR* nu mai reprezintă o soluţie la fel de viabilă. Indiferent de costurile procedurii sau de durata în care se ia o soluţie, părţile ar trebui să dorească, în special, soluţionarea temeinică a cauzei şi nu rezolvarea ei cât mai rapid.

2.3.2. Dezavantajele BDR

Deciziile sunt luate, în cadrul acestei metode, de către mai multe persoane şi acest lucru reprezintă, la o primă vedere, un avantaj, mulţi autori făcând inclusiv referire, aşa cum am arătat mai sus, şi la termenul de *wisdom of the crowd*[50]. Dar, deciziile nu sunt luate în urma consultării dintre utilizatori. Între aceştia nu există nicio formă de dialog pe toată durata procedurii şi, astfel, din moment ce ei nu se pot influenţa reciproc, metoda de soluţionare nu apelează cu adevărat la *înţelepciunea utilizatorilor*. O decizie colectivă presupune o colaborare între persoanele ce urmează să o ia, iar în cazul în care există opinii divergente, ele pot încerca să se influenţeze reciproc, dar acest lucru este exclus în cadrul *BDR*. În situaţia în care decizia este luată, prin vot majoritar, dar fără ca decidenţii să se poată consulta, aceasta nu mai este una colectivă. Deşi utilizatorii nu comunică între ei în timpul deliberării, acest lucru nu presupune în mod automat că decizia este una greşită, dar, din moment ce ei nu încearcă să ajungă la un punct comun, cresc şansele ca decizia să nu fie corectă[51]. Spre exemplu, în cadrul *Kleros*, deciziile sunt luate fără ca utilizatorii să poată comunica între ei iar modul în care ei sunt remuneraţi chiar încurajează această lipsă de comunicare[52].

În cazul soluţionării unui litigiu de către instanţele statale sau arbitrale, legitimitatea soluţiilor este generată şi de imparţialitatea judecătorilor sau a arbitrilor. În cadrul procedurilor desfăşurate în faţa instanţelor statale, atunci când judecătorul nu oferă suficiente garanţii referitoare la imparţialitatea sa, oricare

[49] *Ibidem.*
[50] A. Gudkov, *op. cit.*, p. 65.
[51] *Idem*, p. 69.
[52] A se vedea *infra*, *2.4. Modul în care sunt soluţionate litigiile în cadrul platformei Kleros.*

dintre părţi poate formula o cerere de recuzare împotriva acestuia[53]. Inclusiv arbitrii aleşi să soluţioneze un litigiu pot fi înlocuiţi în cazul în care nu oferă toate garanţiile cu privire la imparţialitatea sau la independenţa lor[54].

Spre deosebire de aceste situaţii, în cadrul *BDR*, părţile nici nu cunosc persoana celui ce soluţionează litigiul. Utilizatorii se diferenţiază unul de celălalt prin intermediul *crypto adresei*. Dar, un utilizator poate avea mai multe astfel de adrese şi, astfel, se poate înrola în cadrul unei platforme de mai multe ori şi, dacă este repartizat, poate să soluţioneze un litigiu ca şi cum decizia ar fi luată de mai multe persoane. Asemenea acţiuni sunt cunoscute şi sub numele de *sybil attacks*[55]. Lipsa oricărui mecanism de verificare a utilizatorilor nu oferă nicio garanţie celor ce doresc soluţionare litigiilor prin această procedură că nu se vor confrunta cu o asemenea problemă[56].

Pe lângă riscul ca un singur utilizator să soluţioneze un litigiu folosind mai multe *crypto adrese*, din cauza faptului că utilizatorii sunt anonimi, există un risc şi mai mare cu privire la influenţarea lor de către una dintre părţi. Tocmai şi din acest motiv, *Kleros* oferă posibilitatea părţilor de a ataca hotărârea luată de către utilizatori, iar în cadrul căii de atac numărul acestora se va majora, acest lucru oferind o protecţie suplimentară împotriva influenţării utilizatorilor de către părţi[57].

Un alt dezavantaj este reprezentat de faptul că litigiile tind să fie soluţionate fără ca utilizatorii să interpreteze sau să aplice nicio normă de drept. Astfel, în cadrul comunităţilor *blockchain*, părţile unui litigiu provin, cel mai probabil, din state diferite. În mod normal, acest lucru ar aduce modificări foarte importante litigiului, modificări reprezentate, în special, de modul în care părţile au ales sau nu o lege aplicabilă litigiului şi o instanţă competentă. Dar, în cadrul unor asemenea comunităţi, oricum există o încercare de a limita cât mai mult ordinea statală şi,

---

[53] Conform art. 44 alin. (1) din Legea nr. 134/2010 privind Codul de procedură civilă (republicată în M. Of. al României, Partea I, nr. 247 din 10 aprilie 2015), *„judecătorul aflat într-o situație de incompatibilitate poate fi recuzat de oricare dintre părți înainte de începerea oricărei dezbateri.*".

[54] În cadrul procedurilor arbitrale desfășurate în fața Curții Internaționale de Arbitraj de la Paris, părțile pot formula o cerere de recuzare împotriva unui arbitru atunci când acestea consideră că există suspiciuni referitoare la lipsa sa de imparțialitate sau de independență. A se vedea, *2021 Arbitration Rules and 2014 Mediation Rules*, p. 26, [Online] la https://iccwbo.org/content/uploads/ sites/ 3/2020/12/icc-2021-arbitration-rules-2014-mediation-rules-english-version.pdf, accesat 21.11.2021.

[55] În general, un astfel de atac presupune activitatea prin care un utilizator al unei platforme își creează multiple conturi de acces în cadrul acesteia și urmărește să influențeze modul în care platforma funcționează. În cadrul *blockchain*-ului, un astfel de atac presupune, de regulă, activitatea prin care o persoană urmărește să dețină controlul asupra mai multor calculatoare interconectate din baza de date și, astfel, să modifice informațiile stocate. A se vedea, *Sybil Attacks Explained*, [Online] la https://academy.binance.com/en/articles/sybil-attacks-explained, accesat 21.11.2021.

[56] A. Gudkov, *op. cit.*, p. 71.

[57] *Idem*, p. 72.

astfel, nici nu prezintă importanţă pentru cei ce soluţionează litigiul faptul că părţile provin din state diferite. Mai grav este faptul că, uneori, contractul dintre părţi chiar conţine o clauză de alegere a legii aplicabile, dar utilizatorii platformei nu ţin cont de aceasta şi soluţionează litigiul conform convingerilor proprii, ceea ce este de aşteptat, din moment ce nu toate persoanele ce se înrolează în cadrul acestor platforme au şi cunoştinţe juridice[58].

Un alt dezavantaj este reprezentat de faptul că nu întotdeauna grăbirea sau accelerarea unei proceduri este şi eficientă. Din moment ce decizia pronunţată este una greşită, nu mai prezintă un avantaj soluţionare acesteia în regim de urgenţă. Principalul scop ar trebui să fie în continuare acela de a afla adevărul în cauză pentru a putea, ulterior, să fie soluţionată problema într-un mod corect. Astfel, în cadrul acestor proceduri, de cele mai multe ori nici nu sunt administrate probe, iar un litigiu în care nu sunt administrate probe nu poate fi soluţionat în mod temeinic. Din acest punct de vedere, este bine că se are în vedere celeritatea unei proceduri, dar acest lucru nu trebuie făcut în detrimentul aflării adevărului. Desigur, părţile îşi asumă toate aceste riscuri în momentul în care stabilesc de comun acord să recurgă la o asemenea procedură, iar faptul că obiectul litigiului are, de cele mai multe ori, o valoare redusă nu face decât să diminueze din riscurile asumate[59].

2.4. Modul în care sunt soluţionate litigiile în cadrul platformei *Kleros*

Platforma *Kleros* a fost aleasă, ca studiu de caz, din două motive. În primul rând, este cea mai dezvoltată platformă *BDR* ce oferă acces oricărei persoane interesate, nelimitând-se la o comunitate deja existentă în cadrul său[60].

În al doilea rând, *Kleros* prezintă relevanţă datorită faptului că, în octombrie 2021, o instanţă statală din Mexic a recunoscut o procedură arbitrală desfăşurată în cadrul platformei, ceea ce demonstrează utilitatea şi importanţa *Kleros*. În acest sens, în anul 2020, într-un contract de leasing încheiat în Mexic, a fost introdusă o clauză arbitrală ce stabilea ca orice litigiu ulterior izvorât din acest contract să fie soluţionat de către un singur arbitru ales de către părţi. Totodată, clauza arbitrală stabilea şi modul în care urma să aibă loc procedura arbitrală, făcând referire la regulile platformei *Kleros*. La momentul apariţiei disputei, arbitrul desemnat de către părţi a trimis toate datele necesare platformei, iar, în cadrul acesteia, trei utilizatori au soluţionat litigiul. Pe baza deciziei luate de *Kleros*, arbitrul a pronunţat hotărârea arbitrală, iar, ulterior, în cadrul procedurii de recunoaştere a hotărârii, instanţa statală a recunoscut hotărârea pronunţată de arbitru în baza deciziei luate de platformă[61].

[58] A. Gudkov, *op. cit.*, p. 73.

[59] A. Gudkov, *op. cit.*, p. 74.

[60] În acest sens, în cadrul *Kleros* își desfășoară activitatea, la momentul redactării acestui articol, 767 de *juraţi*, aceştia soluționând de-a lungul timpului peste 1000 de litigii. A se vedea, [Online] la https://kleros.io/, accesat 30.11.2021.

[61] M.V. Carrera, *Accommodating Kleros As A Decentralised Dispute Resolution Tool For Civil Justice Systems: Theoretical Model And Case Of Application*, p. 16, [Online] la

Cel mai probabil, hotărârea instanţei statale s-a bazat pe hotărârea pronunţată de arbitru şi nu pe decizia luată în cadrul platformei. De altfel, o astfel de decizie nici nu are cum să facă obiectul unei proceduri de recunoaştere în faţa unei instanţe statale. Dar, chiar şi aşa, hotărârea luată de către instanţa din Mexic prezintă importanţă pentru adepţii şi utilizatorii acestei modalităţi alternative de soluţionare a litigiilor.

Conform propriei descrieri, platforma *Kleros* reprezintă un spaţiu dedicat soluţionării alternative a litigiilor prin utilizarea *blockchain*-ului, ce oferă, prin intermediul serviciilor sale, o cale rapidă şi uşor de accesat pentru soluţionarea litigiilor în mediul online. Sintetizând modul în care este luată o decizie în cadrul *Kleros*, atunci când o problemă necesită a fi soluţionată, platforma apelează la utilizatorii înrolaţi în cadrul său (platforma foloseşte termenul de *jurors* – juraţi). Aceştia sunt traşi la sorţi, prin utilizarea unui algoritm, pentru a le fi repartizat respectivul litigiu şi, ulterior, *juraţii* iau o decizie în mod individual, fără a se consulta unul cu celălalt. Hotărârea este luată cu majoritatea voturilor exprimate. Utilizatorii ce au votat conform votului majoritar sunt remuneraţi, iar celorlalţi le este luată din propriul cont o anumită valoare calculată în *cryptomoneda* platformei. Odată luată, decizia este pusă în executare prin intermediul unui *smart contract* încheiat în momentul în care părţile au decis să recurgă la serviciile platformei[62].

Atât numele *Kleros*, cât şi denumirea *cryptomonedei*, *Pinakion*, sunt preluate din sistemul folosit în Atena antică prin care erau selectaţi cei ce urmau să soluţioneze o problemă importantă pentru comunitate. Aceştia erau aleşi prin intermediul unui dispozitiv (un bloc de piatră), denumit *kleroterion*, în care cei ce doreau puteau introduce o plăcuţă ce conţinea numele lor, aceasta fiind denumită *pinakia*[63].

Asemănările dintre platformă şi sistemul folosit în Atena acum 2000 de ani se opresc aici. Astfel, pentru ca un utilizator să poată să se înroleze în cadrul *Kleros*, el trebuie, mai întâi, să achiziţioneze o anumită valoare de *cryptomonedă* şi să depună această valoare în cadrul secţiunilor specializate din cadrul platformei[64]. Fiecare secţiune specializată (platforma foloseşte termenul de *instanţă specializată*)

---

https://ipfs.kleros.io/ipfs/QmfNrgSVE9bb17KzEVFoGf4KKA1Ekaht7ioLjYzheZ6prE/Accommodating%20Kleros%20as%20a%20Decentralized%20Dispute%20Resolution%20Tool%20for%20Civil%20Justice%20Systems%20-%20Theoretical%20Model%20and%20Case%20of%20Application%20-%20Mauricio%20Virues%20-%20Kleros%20Fellowship%20of%20Justice.pdf, accesat 23.11.2021.

[62] M. Dylag, H. Smith, *op. cit.*, p. 6.

[63] *Idem*, p. 8; *Kleroterion – Ensuring a Just Democracy*, [Online] la https://joyofmuseums.com/museums/europe/greece-museums/athens-museums/museum-of-the-ancient-agora/kleroterion/, accesat 25.11.2021; F. Ast, A. Sewrjugin, *CrowdJury, a crowdsourced justice system for the collaboration era*, p. 3, [Online] la https://www.researchgate.net/publication/283687907_CrowdJury_a_crowdsourced_justice_system_for_the_collaboration_era, accesat 25.11.2021.

[64] În momentul de faţă există opt secţiuni specializate, cărora li se alătură secţiunea ce are rolul de a soluţiona căile de atac împotriva soluţiilor luate de către oricare dintre acestea. [Online] la https://court.kleros.io/courts, accesat 25.11.2021.

prevede un prag diferit de *cryptomonedă* ce trebuie depusă. Odată ce este îndeplinită această condiţie, utilizatorii pot fi traşi la sorţi pentru a dobândi calitatea de jurat. Dar, modul în care sunt repartizaţi nu este neapărat unul aleatoriu. Inclusiv *Kleros* afirmă că utilizatorii ce au depus mai multă *cryptomonedă* au şanse mai mari de a fi traşi la sorţi. Fiind avantajaţi aceştia, platforma determină, indirect, o circulaţie sporită a propriei monede virtuale, crescând-i astfel valoarea[65].

În momentul în care au fost traşi la sorţi, utilizatorilor li se blochează o anumită valoare de monedă virtuală. Ulterior, aceştia trebuie să soluţioneze litigiul şi în funcţie de votul majoritar şi de votul lor, respectiva sumă le este sau nu deblocată. Dacă votul acestora este conform votului majorităţii, suma le este deblocată şi, totodată, ei primesc şi un spor de eficienţă, dar dacă ei se află în minoritate, pierd suma blocată de către platformă. Practic, fiecare trebuie să identifice o soluţie în mod individual şi să mizeze pe faptul că şi ceilalţi vor ajunge la aceeaşi concluzie[66].

Cu privire la acest mod de luare a deciziilor şi de remunerare a juraţilor sunt necesare câteva precizări. În primul rând, utilizatorii nu sunt remuneraţi în funcţie de munca depusă, ci în funcţie de decizia propusă. Practic, juraţii speculează care va fi decizia majoritară şi se aliniază acesteia. Acţiunea lor se aseamănă mai mult unei specule, decât unui mod de a soluţiona un litigiu în mod echitabil, ei urmărind să obţină un folos patrimonial, dar nu prin munca depusă, ci prin intermediul gradului de predictibilitate al soluţiei luate. În al doilea rând, din cauza modului în care sunt remuneraţi utilizatorii este pusă sub semnul întrebării corectitudinea deciziei luate. Ne putem imagina situaţia unui litigiu complex în care soluţia este mult mai greu de identificat. Iar o persoană care are cunoştinţe peste medie nu va vota conform propriilor convingeri, deoarece ea trebuie, practic, să intuiască care va fi decizia majoritară. Astfel, ea nu îşi va susţine punctul de vedere (ce poate fi corect) şi se va alinia unui punct de vedere majoritar deoarece urmăreşte să obţină profit din această acţiune.

Pe lângă discuţiile legate de corectitudinea deciziei, trebuie făcută o precizare şi cu privire la scopul urmărit de platformă. Prin modalitatea de atribuire a cauzelor utilizatorilor şi prin modalitatea de luare a deciziilor, *Kleros* urmăreşte creşterea circulaţiei propriei monede virtuale şi, astfel, creşterea valorii acesteia. Tocmai şi din această cauză le sunt atribuite cu precădere litigii pentru soluţionare utilizatorilor ce au depus mai multă *cryptomonedă*. Practic, majoritatea platformele *BDR*, nu doar *Kleros*, depind de gradul de circulaţie al monedelor virtuale create de către acestea[67].

[65] M. Dylag, H. Smith, *op. cit.*, p. 8.
[66] M. Dylag, H. Smith, *op. cit.*, p. 9.
[67] *Idem, p.* 11.

Concluzii

Mijloacele alternative de soluţionare a litigiilor au fost puternic influenţate de evoluţia tehnologică şi de expansiunea Internetului, iar utilizarea *blockchain* în soluţionare litigiilor nu vine decât să aducă un spor de noutate acestui domeniu.

Modul în care comunităţile *blockchain* regândesc actul de justiţie este unul inovativ. Practic, actul de justiţie este realizat, în cadrul acestor *ecosisteme*, prin intermediul *crypto instanţelor* ce iau hotărâri într-un mod descentralizat şi pun în executare hotărârile prin intermediul unor *smart contracts*.

Dar, nu orice noutate este şi eficientă. Deşi prezintă unele avantaje, utilizarea *blockchain* în soluţionarea litigiilor naşte, în mod clar, şi suficiente probleme. Din acest punct de vedere, indiferent cât de bine ar fi structurat un algoritm sau cât de bine pregătiţi ar fi unii utilizatori ai platformelor, ei nu se pot substitui în sarcinile unui judecător sau ale unui arbitru. Chiar şi dacă respectivii judecători sau arbitri pot greşi, indiferent cât se încearcă, inteligenţa artificială nu poate înlocui întrutotul factorul uman.

Dar asta nu înseamnă că tehnologia *blockchain* nu poate fi şi utilă. Ideal ar fi ca aceasta să fie utilizată cu scopul de a facilita procesul de soluţionare a unui litigiu şi nu cu scopul de a înlătura factorul uman decident. Iar, în aceste condiţii, progresul tehnologic nu poate fi decât unul de bun augur.

Totodată, asemenea tuturor domeniilor în care a fost utilizat *blockchain*-ul, viitorul acestui mod de soluţionare a litigiilor depinde, în primul rând, de utilizatorii platformelor. Cu cât există mai mulţi adepţi ai acestui mijloc, cu atât sunt mai multe şanse ca el să aibă succes pe termen lung.

Referinţe

Ast F., Sewrjugin A., *CrowdJury, a crowdsourced justice system for the collaboration era*, [Online]

Barnett J., Treleaven P., *Algorithmic Dispute Resolution – The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies*, în The Computer Journal, Section C: Computational Intelligence, Machine Learning and Data Analytics, Vol. 61, Nr. 3, 2018, DOI: https://doi.org/10.1093/comjnl/bxx103

Carrera M.V., *Accommodating Kleros As A Decentralised Dispute Resolution Tool For Civil Justice Systems: Theoretical Model And Case Of Application*, [Online]

Dimov D., *Crowdsourced online dispute resolution*, în Leiden University Center for Law and Digital Technologies, [Online]

Dylag M., Smith H., *From cryptocurrencies to cryptocourts: blockchain and the financialization of dispute resolution platforms*, în Information, Communication & Society, [Online]

Gonzales W., Masumy N., *Online Dispute Resolution Platforms: Cybersecurity Champions in the COVID-19 Era? Time for Arbitral Institutions to Embrace ODRs*, în Kluwer Arbitration Blog, [Online]

Gudkov A., *Crowd Arbitration: Blockchain Dispute Resolution*, în Legal Issues in the Digital Age, Nr. 3, 2020, DOI: https://doi.org/10.17323/2713-2749.2020.3.59.77

Gupta V., *A Brief History of Blockchain*, în Harvard Business Review, [Online]

Raymond A.H., Shackelford S.J., *Technology, Ethics, and Access to Justice: Should an Algorithm be Deciding Your Case?*, în Michigan Journal of International Law, Vol. 35, Nr. 3, 2014, [Online]

Rosencrance L., Loshin P., Cobb M., *Two-factor authentication (2FA)*, [Online]

Seth S., *UK Courts Start Pilot Blockchain Evidence System*, [Online]

Stângaciu R.D., *Limite ale implicării tehnologiei în soluționarea prin mijloace alternative a litigiilor Online Dispute Resolution prin prisma raporturilor de comerț internațional*, în Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" Iaşi, Tomul LXV, Ştiinţe Juridice, 2019, Supliment, [Online]

Ungureanu C.T., *Dreptul comerţului internaţional*, Editura Hamangiu, Bucureşti, 2018

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII SUPLIMENT 2, ŞTIINȚE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-11

Executarea acordurilor încheiate prin mijloace electronice rezultate din mediere în litigiile de comerţ internaţional în baza Convenţiei de la Singapore

Enforcement of Settlement Agreements Resulting from Mediation Concluded by Electronic Communication in International Trade Disputes under the Singapore Convention

Ionela-Diana Pătraşc-Bălan[1]

Rezumat: Principala reticienţă a părţilor în a soluţia litigiile de comerţ internaţional prin mediere a fost lipsa forţei executorii a acordului de mediere. *The United Nations Convention on International Settlement Agreements Resulting from Mediation (the Singapore Convention),* Convenţia Naţiunilor Unite cu privire la acordurile internaţionale rezultate din mediere (Convenţia de la Singapore) este primul instrument multilateral care reglementează problematica referitoare la recunoaşterea şi executarea acordurilor de mediere internaţionale încheiate în materie comercială. Prin prezentul articol ne propunem să analizăm condiţiile în care un acord de mediere şi, în particular, un acord de mediere încheiat prin mijloace electronice poate fi pus în executare conform Convenţiei de la Singapore.

Cuvinte-cheie: Convenţia de la Singapore; acord de mediere; mijloace electronice; punere în executare

Abstract: The main reluctance of the parties to resolve international trade disputes through mediation was the lack of enforceability of settlement agreement resulting from mediation. The United Nations Convention on International Settlement Agreements Resulting from Mediation (the Singapore Convention) is the first multilateral instrument to regulate the recognition and enforcement of international settlement agreements resulting from mediation concluded in commercial matters. This article aims to examine the conditions under which a settlement agreement resulting from mediation and, in particular, a settlement agreement concluded by electronic communication is enforceable in accordance with the Singapore Convention.

Keywords: Singapore Convention; settlement agreement resulting from mediation; electronic communication; enforceability

[1] Doctorand, Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iaşi, e-mail: dianapat27@yahoo.com.

1. Introducere

Pentru soluţionarea diferendelor ivite în executarea relaţiilor comerciale internaţionale părţile au la dispoziţie mai multe mijloace[2]: negocierea, modalitate de rezolvare a neînţelegerilor prin discuţii directe; medierea/concilierea sau alte forme de soluţionare voluntară asimilate, intermediate de un terţ care asistă şi ajută părţile să ajungă la o înţelegere; arbitrajul, procedură care se desfăşoară prin intermediul unui tribunal arbitral şi se finalizează cu o decizie obligatorie; instanţele de judecată care pronunţă hotărâri obligatorii pentru litiganţi.

Printre elementele care diferenţiază aceste modalităţi de rezolvare a diferendelor putem identifica caracterul executoriu al actului final al procedurii de soluţionare a diferendelor, executorialitatea fiind prezentă în cazul hotărârilor arbitrale şi a celor judecătoreşti. Potrivit unui studiu realizat de *Singapore International Dispute Resolution Academy* (SIDRA), principalul criteriu în alegerea unui mijloc de soluţionare a litigiilor pentru 71% dintre respondenţi îl reprezintă forţa executorie a hotărârii prin care se soluţionează diferendul[3].

Medierea este inclusă în categoria mijloacelor alternative de soluţionare a litigiilor[4]. Indiferent dacă medierea este *ad-hoc* sau instituţionalizată, desfăşurată prin intermediul unui centru de arbitraj, acest mijloc de soluţionare a neînţelegerilor dintre părţi presupune intervenţia unui terţ al cărui rol este acela de a le asista în încercarea de a ajunge la un acord de soluţionare, de a facilita semnarea acordului, fără a putea impune o soluţie[5].

---

[2] J. W. Salacuse, *Is There a Better Way? Alternative Methods of Treaty-Based, Investor-State Dispute Resolution*, în Fordham International Law Journal, Volume 31, Issue 1 2007 Article 6, p. 154, [Online] la https://core.ac.uk/download/pdf/144226963.pdf, accesat 20.09.2021.

[3] *SIDRA International Dispute Resolution Survey: 2020 Final Report*, p. 7, [Online] la https://sidra.smu.edu.sg/sites/sidra.smu.edu.sg/files/survey/50/index.html, accesat 12.09.2021.

[4] Conform SIDRA, *op. cit.*, p. 7, sintagma „mijloace alternative de soluționare a litigiilor" (*Alternative Dispute Resolution, ADR*) a început să fie utilizată la mijlocul anilor 1970 în Statele Unite ale Americii; Într-o accepțiune exprimată de S.D. Franck, *Challenges Facing Investment Disputes: Reconsidering Dispute Resolution in International Investment Agreements. Appeals mechanisms in international investment disputes, Karl P. Sauvant, ed., Oxford University Press, 2008, Washington & Lee Legal Studies Paper No. 2009-03*, p. 158, [Online] la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1427590, accesat 22.02.2021, în ADR sunt incluse modalități de soluționare a litigiilor altele decât prin intermediul instanțelor; Într-o a doua interpretare exprimată în United Nations Conference On Trade And Development, *Investor-State Disputes: Prevention and Alternatives to Arbitration II,* United Nations New York and Geneva, 2011, p. xii, [Online] la https://unctad.org/system/files/official-document/webdiaeia20108_en.pdf, accesat 18.02.2021, prin ADR se înțelege modalitatea de rezolvare a diferendelor dintre părți, alta decât metodele primare de soluționare a disputelor, respectiv procedurile desfășurate în fața instanțelor de judecată statale sau în față instanțelor arbitrale internaționale.

[5] *Idem;* C. Kessedjian*, Droit du commerce international,* Ed. Presse Universitaires de France, Paris, 2013, p. 447*;* C.T. Ungureanu, *Enforcement of the post- mediation agreement in*

O mediere de succes se finalizează prin încheierea unei înţelegeri numită acord de mediere. Deşi avantajele medierii faţă de celelalte metode de soluţionare a litigiilor de comerţ internaţional sunt recunoscute (costuri financiare şi durată de soluţionare reduse, păstrarea relaţiilor dintre contractanţi, confidenţialitate, libertatea de a alege regulile de procedură)[6], principalul său dezavantaj a fost identificat ca fiind lipsa forţei executorii a acordului de mediere[7], precum şi inexistenţa unui cadru juridic internaţional unitar pentru punerea în executare a acordurilor de mediere[8] .

În legislaţiile care reglementează soluţionarea litigiilor prin mediere, acordul de mediere are natura juridică a unui contract[9]. Această calificare lipseşte acordul de mediere de forţa executorie a unei sentinţe arbitrale sau a unei hotărâri judecătoreşti. Acordul de mediere rezultat în urma soluţionării unui litigiu comercial internaţional nu poate fi recunoscut sau pus în executare direct în temeiul instrumentelor internaţionale care reglementează domeniul recunoaşterii şi executării sentinţelor arbitrale străine sau a hotărârilor judecătoreşti străine, respectiv Convenţia Naţiunilor Unite pentru recunoaşterea şi executarea sentinţelor arbitrale străine încheiată la New York în 1958 (Convenţia de la New York)[10], Convenţia din 18 martie 1965 pentru reglementarea diferendelor relative la investiţii între state şi persoane ale altor state (Convenţia de la Washington)[11], Convenţia din 30 iunie 2005 privind acordurile de alegere a forului (Convenţia de la Haga)[12].

---

international trade disputes, în Modernizarea legislației naționale în contextul uniformizării dreptului la nivel european și implicațiile socio-politice asupra sistemului administrativ, Editura Hamangiu, București, 2014, p. 279.

[6] C. Kessedjian, *op. cit.,* p. 447; C.T. Ungureanu, *op. cit.*, p. 279; T. Schnabel, *The Singapore Convention on Mediation: A Framework for the Cross-Border Recognition and Enforcement of Mediated Settlements* (September 18, 2018). 19 Pepp. Disp. Resol. L.J. 1 (2019), [Online] la https://ssrn.com/abstract=3239527 or http://dx.doi.org/10.2139/ssrn.3239527, p. 2, accesat 13.02.2021; M. Sîrbu, *Metodele ADR în contextul european și internațional*, Editura Universul Juridic, București, 2020, pp. 78-79.

[7] J. W. Salacuse, *op. cit.*, p. 179; C.T. Ungureanu, o*p. cit.,* p. 280; T. Schnabel, *op. cit.*, p. 2; M. Sîrbu, *op. cit.*, p. 131.

[8] C. Jura, *O introducere în materia Convenţiei Naţiunilor Unite privind Acordurile Internaţionale Rezultate în urma Medierii – Convenţia de la Singapore,* în Revista română de arbitraj nr. 1/2020, [Online] la https://sintact.ro/#/publication/151017435?keyword=conventia%20de%20la%20singapore&cm=SREST, accesat 12.09.2021.

[9] C. Kessedjian, *op. cit.*, p. 451; C.T. Ungureanu, *Punerea în executare …, op. cit.,* p. 280.

[10] Textul convenției este disponibil [Online] la https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/new-york-convention-e.pdf, accesat 28.10.2021; România a aderat la această convenție prin Decretul nr. 186/10.06.1968 publicat în B.O. nr. 19 din 24.07.1961.

[11] Textul convenției este disponibil [Online] la https://icsid.worldbank.org/sites/default/files/ICSID%20Convention%20English.pdf, accesat 28.10.2021.

[12] Textul convenției este disponibil [Online] la https://op.europa.eu/ro/publication-detail/-/publication/196d3251-fa6f-11e7-b8f5-01aa75ed71a1/language-ro, accesat 28.10.2021; UE a semnat Convenția de la Haga prin Decizia Consiliului din 26 februarie 2009

În practică, pentru a înlătura acest dezavantaj, s-a apelat la o ficţiune juridică. În situaţia în care părţile au ajuns la încheierea unui acord de mediere după regulile elaborate şi propuse de ICSID, pentru a suplini lipsa caracterului executoriu al acordului de mediere, a fost avansată ipoteza încorporării sale într-o sentinţă arbitrală conform art. 43 alin. (2) din *ICSID Arbitration Rules*[13]. În această modalitate, acordul de mediere putea beneficia de procedura mecanismului de executare a Convenţiei de la Washington. Cu toate acestea, rămânea deschisă problematica referitoare la compatibilitatea utilizării unei proceduri similare de pronunţare a unei sentinţe cu privire la acordul de mediere (numirea mediatorului arbitru *ad-hoc* şi inserarea acordului de mediere în cuprinsul unei sentinţe arbitrale) cu mecanismul de punere în executare a sentinţelor arbitrale în baza Convenţiei de la New York[14]. În spaţiul UE, acordurile de mediere transfrontalieră care îmbracă forma unui înscris notarial sau a unei hotărâri judecătoreşti prin care s-a luat act de înţelegerea părţilor pot fi puse în executare în temeiul Regulamentul (UE) nr. 1215/2012 al Parlamentului European şi al Consiliului din 12 decembrie 2012 privind competenţa judiciară, recunoaşterea şi executarea hotărârilor în materie civilă şi comercială (Regulamentul (UE) nr. 1215/2012)[15].

Pentru a înlătura principalul dezavantaj al utilizării medierii ca mijloc alternativ de soluţionare a litigiilor de comerţ internaţional a fost adoptată la 20 decembrie 2018 *United Nations Convention on International Settlement Agreements Resulting from Mediation (Singapore Convention on Mediation, Singapore*

privind semnarea în numele Comunității Europene a Convenției privind acordurile de alegere a forului, publicat în OJ L 133, 29.5.2009; UE a aprobat Convenția de la Haga prin Decizia Consiliului din 4 decembrie 2014 cu privire la aprobarea, în numele Uniunii Europene, a Convenției de la Haga din 30 iunie 2005 privind acordurile de alegere a forului, publicată în OJ L 353, 10.12.2014. Convenția de la Haga a intrat în vigoare la 1 octombrie 2015.

[13] Art. 43 alin. (2) din *ICSID Arbitration Rules; ICSID Arbitration Rules* pot fi consultate [Online] la https://icsid.worldbank.org/resources/rules-and-regulations/convention/arbitration-rules, accesat 30.09.2021.

[14] B.L. Steele, *Enforcing International Commercial Mediation Agreements as Arbital Awards Under the New York Convention* în 54 UCLA Law Review 1385 (2007), pp. 1397-1399, [Online] la https://www.uclalawreview.org/enforcing-international-commercial-mediation-agreements-as-arbital-awards-under-the-new-york-convention/, accesat 30.09.2021; E. Sussman, *The New York Convention Through a Mediation Prism,* în Dispute Resolution Magazine Volume 15, Number 4, Summer 2009, [Online] la https://sussmanadr.com/docs/NY%20Coinvention%20Prism%20ABA%20DR%20as%20printed-%20white%20background%208-09.pdf, accesat 30.09.2021.

[15] Publicat în JO L 351, 20.12.2012; Textul regulamentului este disponibil la adresa https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX%3A32012R1215, accesat 28.10.2021; Pentru executarea acordului de mediere în UE, a se vedea C.T. Ungureanu, *Punerea în executare …*, *op. cit.*, pp. 282-283.

Convention), Convenţia Naţiunilor Unite cu privire la acordurile internaţionale rezultate din mediere (Convenţia de la Singapore)[16].

2. Convenţia de la Singapore

Acest tratat multilateral se alătură şi întregeşte cadrul juridic internaţional în materia recunoaşterii şi executării actelor finale rezultate în urma soluţionării litigiilor de comerţ internaţional, alcătuit din Convenţia de la New York, care se aplică pentru recunoaşterea şi executarea sentinţelor arbitrale străine şi Convenţia de la Haga din 2005, care reglementează recunoaşterea şi executarea hotărârilor judecătoreşti străine[17].

Scopul principal al Convenţiei de la Singapore este acela de a promova medierea ca mijloc de soluţionare a litigiilor de comerţ internaţional. Preambulul tratatului internaţional reafirmă câteva dintre avantajele certe ale medierii: menţinerea relaţiilor contractuale, facilitarea operaţiunilor de comerţ internaţional, economii în administrarea justiţiei statale[18].

Pe lângă noutatea reglementării domeniului medierii printr-un tratat multilateral, adoptarea Convenţiei de la Singapore marchează încă o premieră: UNCITRAL a dezvoltat într-un pachet legislativ două instrumente cu forţă juridică diferite[19]: convenţia, act normativ obligatoriu şi legea model, reglementare de tip *soft-law*, *UNCITRAL Model Law on International Commercial Mediation and*

[16] Textul Convenției de la Singapore este disponibil [Online] la https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/EN/Texts/UNCITRAL/Arbitration/mediation_convention_v1900316_eng.pdf, accesat 30.10.2021; Inițiativa adoptării acestui instrument internațional a aparținut în anul 2014 Statelor Unite ale Americii care a înaintat propunerea privind promovarea sa în contextul dezbaterii privind transparența în arbitrajele investiționale în interiorul Grupului de lucru II din cadrul UNCITRAL. Deși în cadrul discuțiilor purtate pentru adoptarea Convenției de la Singapore, UE și unele SM s-au opus proiectului, acesta a fost adoptat în cele șase sesiuni de lucru ale grupului de lucru dedicate acestui subiect; A se vedea în acest sens, T. Schnabel, *op. cit.*, p. 4. La data deschiderii pentru semnare, Convenția a fost semnată de 46 de state incluzând primele două cele mai mari economii mondiale (SUA și China). Convenția de la Singapore a intrat în vigoare la 12 septembrie 2020. Până la 30 octombrie 2021, această convenție a fost semnată de 55 de state și ratificată de către opt dintre acestea. Lista statelor semnatare părți la Convenție este disponibilă [Online] la https://www.singaporeconvention.org/jurisdictions, accesat 30.10.2021.

[17] La 2 iulie 2019 a fost încheiată *Convention on the recognition and enforcement of foreign judgments in civil or commercial matters.* Textul Convenției este disponibil [Online] la https://assets.hcch.net/docs/806e290e-bbd8-413d-b15e-8e3e1bf1496d.pdf, accesat 30.10.2021. La acest moment, această convenție nu a intrat în vigoare.

[18] Preambulul Convenției de la Singapore, al treilea alineat.

[19] T. Schnabel, *op. cit.*, p. 7.

International Settlement Agreements Resulting from Mediation, 2018[20]. Aceste două reglementări se aplică complementar[21].

Adoptată inițial în anul 2002 sub titulatura *Model Law on International Commercial Conciliation,* actuala formă a Legii model modificată în anul 2018 aduce în plus, pe lângă o schimbare de terminologie (termenul „conciliere" a fost înlocuit cu termenul „mediere"), un capitol ce se referă la acordurile internaţionale de mediere şi punerea lor în executare. Scopul noii versiunii a Legii model a fost acela de ajuta statele să adopte sau să îşi modernizeze legislaţia în materia medierii, şi, totodată, de a fi un instrument util în aplicarea Convenţiei de la Singapore[22]. UE a susţinut această modificare a Legii model, argumentând că vechea formă din 2002 conţinea reglementări care veneau în contradicţie cu Directiva 2008/52/EC[23].

2.1. Punerea în executare a acordului rezultat din mediere

În temeiul Convenţiei de la Singapore, acordul de mediere va putea fi pus în executare pe teritoriul unui stat parte la această convenţie printr-o procedură similară punerii în executare a unei hotărâri arbitrale străine sau unei hotărâri judecătoreşti străine, conform procedurilor reglementate de Convenţia de la New York, respectiv de Convenţia de la Haga. Operatorii de comerţ internaţional aflaţi în posesia unui acord de mediere se vor adresa direct autorităţilor competente din statul solicitat pentru punerea în executare a acordului de mediere.

În caz de neexecutare, partea interesată poate solicita punerea în executare a acordului de mediere conform art. 3 alin. (1) din Convenţia de la Singapore. Totodată, acordul de mediere poate constitui un mijloc de apărare în cadrul unui litigiu declanşat ulterior asupra unei chestiunii ce a fost tranşată între părţi prin acordul de mediere (art. 3 alin. (2) din Convenţia de la Singapore).

Spre deosebire de Convenţia de la New York care foloseşte în titulatura sa termenul „recunoaşte" şi termenul „executare" în legătură cu sentinţele arbitrale străine, Convenţia de la Singapore nu utilizează sintagma „recunoaşterea acordului

[20] Textul Legii model este disponibil [Online] la https://uncitral.un.org/sites/uncitral.un.org/ files/media-documents/uncitral/en/annex_ii.pdf., accesat 30.10.2021.

[21] N.Y. Morris-Sharma, *Constructing the Convention on Mediation: The Chairperson's Perspective* (2019) 31 Singapore Academy of Law Journal 487-519 p. 29, [Online] la https://journalsonline.academypublishing.org.sg/Journals/Singapore-Academy-of-Law-Journal-Special-Issue/e-Archive/ctl/eFirstSALPDFJournalView/mid/513/ArticleId/1468/Citation/JournalsOnlinePDF, accesat 12.09.2021.

[22] *UNCITRAL Model Law on International Commercial Mediation and International Settlement Agreements Resulting from Mediation, 2018,* [Online] la https://uncitral.un.org/en/texts/mediation/modellaw/commercial_conciliation, accesat 12.09.2021.

[23] N. Alexander, S. Chong, *UN Treaty on mediation signed in Singapore, Nederlands-Vlaams tijdschrift voor mediation en conflictmanagement. 23, (2-3), 71-76, 2019 Singapore Management University School of Law Research Paper No. 14/2020,* p. 75, [Online] la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3583399, accesat 11.09.2021; Directiva 2008/52/CE a Parlamentului European și a Consiliului din 21 mai 2008 privind anumite aspecte ale medierii în materie civilă și comercială, publicată în JO L 136, 24.5.2008.

de mediere". Redactorii tratatului multilateral au optat pentru o abordare funcţională. Prin dispoziţiile art. 3 alin. (2) din Convenţia de la Singapore au fost reglementate efectele instituţiei „recunoaşterii" acordului de mediere, dar nu a fost utilizată *expressis verbis* această noţiune[24]. Soluţia finală este rezultatul opoziţiei manifestate în timpul negocierilor de către unele state, care au argumentat că termenul „recunoaştere" poate fi asociat doar în legătură cu hotărârile judecătoreşti, şi nu în legătură cu înţelegeri dintre particulari, întrucât efectul de *res judicata* poate fi ataşat doar acestora[25]. Aceasta nu semnifică faptul că acordul de mediere nu poate fi recunoscut, întrucât o parte poate invoca acordul de mediere în faţa instanţei pentru a putea dovedi că problema dedusă judecăţii a fost deja soluţionată prin acordul de mediere în situaţia în care este chemată în judecată pentru o chestiune litigioasă dezlegată printr-un acord anterior de mediere[26].

Conform art. 3 pct. 1 din Convenţia de la Singapore care consacră principiul autonomiei procedurale, fiecare stat parte la convenţie va aplica propriile norme de procedură pentru punerea în executare a acordului de mediere în condiţiile prevăzute de tratatul multilateral[27].

2.2. Formalităţi pentru punerea în executare a acordului de mediere

Pentru a pune la dispoziţia părţilor un instrument internaţional flexibil şi atractiv, redactorii Convenţiei de la Singapore au prevăzut condiţii minime în ceea ce priveşte formalităţile pe care părţile trebuie să le îndeplinească pentru executarea acordului de mediere[28].

În vederea punerii în executare, partea interesată va adresa autorităţii competente din statul solicitat parte la Convenţia de la Singapore, care trebuie să fie altul decât statul în care a fost încheiat acordul, o cerere, la care va anexa acordul de mediere semnat de către părţi şi dovada împrejurării că această înţelegere

[24] N.Y. Morris-Sharma, *op. cit.*, p. 500; T. Schnabel, *op. cit.*, p. 37; S. Chong, F. Steffek, *Enforcement of International Settlement Agreement Resulting from mediation under the Singapore Convention* – Private International Law Issues in Perspective", Singapore Academy of Law Volume 31 (2019), p. 465, [Online] la https://journalsonline.academypublishing.org.sg/Journals/Singapore-Academy-of-Law-Journal-Special-Issue/e-Archive/ctl/eFirstSALPDFJournalView/mid/513/ArticleId/1467/Citation/JournalsOnlinePDF., accesat 12.09.2021; K. McCormick, S.S. M. Ong, *"Through the Looking Glass: An Insider's Perspective into the Making of Singapore Convention on Mediation" (*2019) 31 Singapore Academy of Law Journal, p. 534, [Online] la https://journalsonline.academypublishing.org.sg/Journals/Singapore-Academy-of-Law-Journal-Special-Issue/e-Archive/ctl/eFirstSALPDFJournalView/mid/513/ArticleId/1471/Citation/JournalsOnlinePDF, accesat 12.09.2021.

[25] N.Y. Morris-Sharma, *op. cit.*, p. 502; T. Schnabel, *op. cit.*, p. 35.

[26] Art. 3 alin. (2). din Convenţia de la Singapore.

[27] Art. 3 pct. 1 din Convenţia de la Singapore.

[28] D. Q. Anderson, *The Singapore Convention on Mediation: Supplying the Missing Piece of the Puzzle for Dispute Resolution,* p. 11, Forthcoming, Journal of the Malaysian Judiciary (Nov 2020), Singapore Management University School of Law Research Paper No. 1/2020, available at SSRN: https://ssrn.com/abstract=3553739, accesat 30.10.2021.

privind soluţionarea diferendului este rezultată în urma medierii[29]. Astfel cum rezultă din textul reglementării, aceste condiţii sunt limitative. Statele părţi la Convenţia de la Singapore nu pot impune alte condiţii[30].

Dovada că acordul prezentat de către părţi este rezultatul procesului de mediere poate fi făcută în una dintre următoarele modalităţi: a) acordul de mediere să poarte semnătura mediatorului; b) se prezintă un document semnat de către mediator care atestă împrejurarea că medierea a fost efectuată sau c) un certificat de la instituţia care a administrat medierea; d) se poate prezenta orice altă dovadă acceptată de autoritatea competentă a statului în care se solicită executarea acordului de mediere[31].

2.3. Amânarea recunoaşterii sau executării acordului de mediere

Această procedură este prevăzută la art. 6 din Convenţia de la Singapore[32].

În situaţia în care acordul de mediere a cărui recunoaştere sau executare se solicită face obiectul unei acţiuni în faţa instanţelor judecătoreşti, arbitrale sau a unei alte autorităţi competente şi această cerere este de natură să afecteze cererea formulată în temeiul Convenţiei de la Singapore, redactorii tratatului multilateral asupra medierii au prevăzut posibilitatea ca autoritatea competentă căreia i se solicită recunoaşterea sau executarea să poată amâna decizia asupra acestei cereri, solicitând părţii o garanţie adecvată.

Din textul reglementării rezultă împrejurarea că amânarea este o opţiune lăsată la îndemâna autorităţii competente a statului solicitat, şi nu o obligaţie, procedura executării putând continua şi în aceste circumstanţe.

3. Acordurile care pot fi puse în executare în baza Convenţiei de la Singapore

Convenţia de la Singapore nu este incidentă în cazul tuturor acordurilor rezultate din medierea internaţională, domeniul său de aplicare *ratione materiae* şi *ratione temporis* fiind delimitat prin chiar prevederile tratatului internaţional.

3.1. *Ratione materiae*

Convenţia de la Singapore se aplică: „oricărui acord ce rezultă din mediere şi este încheiat în scris de către părţi pentru rezolvarea unui litigiu comercial (acord de soluţionare) care la momentul încheierii este internaţional…”[33].

3.1.1. Acordul trebuie să rezulte din mediere

În ceea ce priveşte terminologia utilizată în cuprinsul Convenţiei de la Singapore, redactorii tratatului au optat pentru un termen „umbrelă”[34]. În

[29] Art. 4 alin. (1) din Convenția de la Singapore.
[30] T. Schnabel, *op. cit.*, p. 32.
[31] Art. 4 alin. (1) lit. b) din Convenția de la Singapore.
[32] Art. 6 din Convenția de la Singapore.
[33] Articolul 1 alin. (1) din Convenția de la Singapore.
[34] *Idem.*

conformitate cu definiţia cuprinsă la art. 2 pct. 3 din Convenţia de la Singapore, medierea desemnează procesul, indiferent de denumirea pe care îl poartă sau izvorul său, prin care părţile încearcă să ajungă la o soluţionare amiabilă a diferendului dintre ele prin intermediul unuia sau mai multor mediatori, care nu pot impune o soluţie părţilor.

Ori de câte ori acordul la care părţile au ajuns nu este rezultatul unei proceduri care să poată fi caracterizată ca fiind o mediere (procedură amiabilă de soluţionare a litigiului, intermediată de un terţ care nu poate impune o soluţie părţilor[35]), Convenţia de la Singapore nu este aplicabilă. Sunt excluse astfel din câmpul său de aplicare acordurile de mediere care au fost încuviinţate de către o instanţă de judecată sau care au fost încheiate în cadrul procedurilor desfăşurate în faţa instanţelor de judecată şi care sunt executorii ca hotărâre judecătorească în statul instanţei care a încuviinţat acordul părţilor (art. 3 lit. a) din Convenţia de la Singapore). Raţiunea instituirii acestei excepţii a fost aceea de a evita suprapunerea cu domeniul de aplicare a Convenţiei de la Haga şi de a nu oferi părţilor posibilitatea de a alege între aceste două instrumente internaţionale[36]. Pentru identitate de raţiune a fost reglementată prin art. 3 lit. b) din Convenţia de la Singapore şi excluderea din domeniul de aplicare a acordurilor care au fost înregistrate şi sunt executorii ca hotărâre arbitrală, fiind avut în vedere, de această dată, domeniul de aplicare a Convenţiei de la New York.

Din perspectiva Convenţiei de la Singapore nu prezintă relevanţă dacă acordul este rezultatul unei medieri *ad-hoc* sau procedura a fost administrată prin intermediul unei instituţii specializate[37], şi nici dacă părţile au recurs la procedura medierii voluntar sau aceasta a fost una obligatorie, impusă prin lege sau de către o instanţă de judecată[38].

În condiţiile dezvoltării soluţionării alternative a litigiilor online, rămâne deschisă întrebarea dacă algoritmilor inteligenţei artificiale prin intermediul cărora sunt soluţionate litigiile online le pot fi acordate valenţe umane, şi măsura în care se poate considera că procedura online a fost intermediată de un mediator[39].

3.1.2. Acordul de mediere să fie încheiat în scris

Acordul de mediere poate fi consemnat într-un înscris sau poate fi încheiat prin mijloace electronice. Oricare dintre aceste două modalităţi îndeplineşte exigenţele Convenţiei de la Singapore.

Conform art. 2 pct. 2 din Convenţia de la Singapore:„ un acord de mediere este încheiat în scris dacă conţinutul său este consemnat sub orice formă”[40].

[35] S. Chong, F. Steffek, *op. cit*, p. 458.

[36] T. Schnabel, *op. cit.*, p. 25.

[37] C. Jura, *op. cit.*.

[38] T. Schnabel, *Implementation of the Singapore Convention: Federalism, Self-Execution, and Private Law Treaties* (January 22, 2019). 30 Am. Rev. Int'l Arb., 265 (2020), p. 267, [Online] la https://ssrn.com/abstract=3320823, accesat 30.10.2021.

[39] *Idem*, pp. 258-259.

[40] Art. 2 pct. 2 teza întâi din Convenţia de la Singapore.

3.1.2.1. Acordul de mediere încheiat prin mijloace electronice

Acordul de mediere poate fi încheiat şi prin mijloace electronice. În viziunea Convenţiei de la Singapore, o comunicare electronică satisface cerinţa formei scrise a acordului de mediere dacă informaţia pe care o conţine este accesibilă ulterior[41].

Definiţia comunicării electronice cuprinse în Convenţia de la Singapore este expresia aplicării principiului echivalenţei funcţionale pe care UNCITRAL a afirmat-o la nivelul reglementărilor sale din domeniul comerţul electronic internaţional[42], fiind o preluare a art. 9 alin. (2) din *United Nations Convention on the Use of Electronic Communications in International Contract*[43]: „o comunicare electronică satisface această cerinţă dacă informaţia pe care o conţine este accesibilă pentru a fi consultată ulterior"[44]. Această abordare o regăsim şi în *UNCITRAL Model Law on International Commercial Mediation and International Settlement Agreements Resulting from Mediation, 2018*[45], dar şi în *UNCITRAL Model Law on International Commercial Arbitration* [46].

Având în vedere aceste constatări, apreciem că prevederile Convenţiei de la Singapore cu privire la forma electronică a acordului internaţional de mediere ar putea fi aplicate având ca model interpretările şi soluţiile jurisprudenţiale existente referitoare la forma electronică a convenţiei arbitrale internaţionale. Conform Ghidului ICCA pentru interpretarea Convenţiei de la New York din 1958[47], cerinţa formei scrise este îndeplinită în cazul tuturor comunicărilor care sunt consemnate în scris.

Se consideră că îndeplineşte cerinţa Convenţiei de la Singapore cu privire la încheierea acordului de mediere în scris printr-un schimb de e-mail-uri între părţi sau împrejurarea în care acordul părţilor nu este cuprins într-un document unic[48]. De asemenea, satisfac exigenţele Convenţiei de la Singapore şi acordurile de mediere rezultate ca urmare a soluţionării litigiului prin intermediul platformelor

[41] Art. 2 pct. 2 teza a doua din Convenția de la Singapore

[42] N.Y. Morris-Sharma, *op. cit.*, p.499.

[43] Convenția a fost adoptată în 23 noiembrie 2005 și a intrat în vigoare la 1 martie 2013. Textul convenției este disponibil [Online] la https://uncitral.un.org/sites/ uncitral.un.org/files/media-documents/uncitral/en/06-57452_ebook.pdf, accesat 10.09.2021; S. Chong, F. Steffek, *op. cit.*, p. 467.

[44] Art. 9 alin. (2) din *United Nations Convention on the Use of Electronic Communications in International Contract.*

[45] Art. 16 alin. 6 din Legea model.

[46] *UNCITRAL Model Law on International Commercial Arbitration* 1985 With amendments as adopted in 2006, [Online] la https://uncitral.un.org/sites/ uncitral.un.org/files/media-documents/uncitral/en/19-09955_e_ebook.pdf, accesat 10.09.2021; Art. 7 alin. (4) din *UNCITRAL Model Law on International Commercial Arbitration 1985 with amendments as adopted in 2006.*

[47] Consiliul internațional pentru arbitraj comercial, *Ghidul ICCA pentru interpretarea Convenției de la New York din 1958, Un ghid pentru Judecători*, p. 53, [Online] la https://cdn.arbitration-icca.org/s3fs-public/document/media_document/icca_guide_ nyc_romanian.pdf, accesat 29.10.2021.

[48] T. Schnabel, *op. cit.*, p. 28.

online (întâlnirile online, *instant text messaging* sau medierea litigiilor care pot avea sau nu la bază algoritmi ai inteligenţei artificiale)[49].

În cazul acordului de mediere încheiat prin mijloace electronice, condiţia semnării de către părţi sau de către mediator este îndeplinită dacă este utilizată o metodă de identificare a părţilor sau a mediatorului pentru a le indica voinţa cu privire la informaţiile conţinute în comunicarea electronică. Metoda utilizată trebuie să fie o metodă potrivită scopului pentru care respectiva comunicare electronică a fost creată sau transmisă, luând în considerare toate circumstanţele, inclusiv orice acord relevant şi trebuie să fie o metodă care îndeplineşte aceste funcţii singură sau împreună cu alte mijloace de probă[50].

3.1.3. Acordul de mediere să soluţioneze un litigiu comercial

Convenţia de la Singapore nu defineşte sintagma „litigiu comercial". În această ipoteză, un instrument util se dovedeşte Legea model. În înţelesul Legii model, termenul „comercial" ar trebui interpretat în sens larg pentru a putea cuprinde chestiuni legate atât de relaţii contractuale, cât şi noncontractuale. Prin relaţii de natură comercială se înţelege, fără a se limita la acestea, furnizarea de bunuri şi servicii, asigurări, servicii de consultanţă, investiţii, operaţiuni bancare, acorduri de exploatare sau concesionare, transportul de mărfuri sau pasageri pe cale maritimă, feroviară, aeriană sau rutieră[51].

Convenţia de la Singapore nu se aplică acordurilor de mediere încheiate pentru a soluţiona un litigiu în care una dintre părţi are calitatea de consumator sau un litigiu referitor la relaţiile de familie, succesiuni sau de dreptul muncii. Această excepţie este reglementată expres prin art. 2 din Convenţia de la Singapore.

3.1.4. Acordul de mediere să soluţioneze un litigiu comercial internaţional

La momentul încheierii acordului de mediere, litigiul pe care îl soluţionează trebuie să fie internaţional[52]. Convenţia de la Singapore utilizează în legătură cu acordul de mediere termenul de „internaţional" şi nu termenul „străin" care figurează în textul Convenţiei de la New York în legătură cu hotărârile arbitrale. Opţiunea redactorilor a avut în vedere împrejurarea că spre deosebire de arbitraj, în cazul medierii nu există un loc al medierii[53].

Criteriile internaţionalităţii litigiului sunt redate în art. 1 din Convenţia de la Singapore. Astfel, litigiul este internaţional în două situaţii: 1) cel puţin două părţi ale acordului de soluţionare a litigiilor au sediul în state diferite sau 2) în

[49] S. Chong, F. Steffek, *op. cit.*, p. 467.

[50] Art. 4 pct. 2 din Convenția de la Singapore.

[51] Nota de subsol 1 din *UNCITRAL Model Law on International Commercial Mediation and International Settlement Agreements Resulting from Mediation*, 2018.

[52] *Idem*, p. 20.

[53] N.Y. Morris-Sharma, *op. cit.,* pp. 498-499; S. Chong, F. Steffek, *op. cit.*, p. 456; N. Alexander, S. Chong, *Why is there no 'seat' of mediation*?, [Online] la https://www.researchgate.net/publication/347130807_Singapore_Convention_Series_Why_is_there_no_%27seat%27_of_mediation, accesat 29.10.2021; T. Schnabel, *Implementation of the Singapore Convention…, op. cit.,* p. 267.

situaţia în care părţile acordului de soluţionare a litigiilor îşi au sediul în acelaşi stat, acesta este diferit fie de statul în care este executată o partea substanţială a obligaţiilor, conform acordului de soluţionare fie de statul cu care obiectul acordului de soluţionare a litigiilor are cea mai mare legătură.

3.2. *Ratione temporis*

Convenţia de la Singapore se va aplica numai acordurilor de mediere care au fost încheiate după data ratificării, acceptării sau aprobării cu sau fără rezerve[54] de către statul parte la tratatul multilateral[55].

Pe cale de consecinţă, la nivel internaţional va continua să existe un regim juridic neunitar cu privire la punerea în executare a acordurilor rezultate din mediere. În cazul statelor părţi la convenţie, acordul de mediere va putea fi pus în executare în condiţiile stipulate de Convenţia de la Singapore. Pentru situaţia în care un stat nu a ratificat, aprobat sau acceptat Convenţia de la Singapore, punerea în executare a acordului de mediere va depinde de legislaţia statului în cauză[56]. Este şi cazul statelor membre (SM) ale Uniunii Europene (UE), întrucât, până în prezent, nici UE ca organizaţie regională, nici unul dintre SM nu au aprobat sau ratificat Convenţia de la Singapore. În spaţiul unional rămân incidente dispoziţiile Directivei 2008/52/CE, astfel cum aceasta fost transpusă în legislaţiile SM[57]. Acordul de mediere va îmbrăca forma juridică a unui contract, care urmează să fie pus în executare urmând regulile oricărui contract[58]. În ceea ce priveşte acordurile de mediere încheiate prin mijloace electronice, având natura juridică a unor contracte, urmează să fie supuse regimului contractelor electronice şi legislaţiei aplicabile în materie în vigoare la data încheierii lor în spaţiul UE[59]. Cuprins într-

[54] Conform art. 8 din Convenția de la Singapore, un stat parte la convenție poate declara că nu va aplica tratatul acordurilor la care este parte el sau oricare entitate publică sau persoane care acționează în numele unei entități publice (art. 8 alin.1) sau va aplica tratatul doar în măsura în care părțile la acordul de mediere vor fi de acord cu aceasta (art. 8 alin. (2)).

[55] Art. 9 din Convenția de la Singapore.

[56] E. Chua, *Enforcement of international mediated settlements without the Singapore convention on mediation*, (2019). *Singapore Academy of Law Journal*. 31, 572-597. Research Collection School Of Law, [Online] la https://ink.library.smu.edu. sg/sol_research/3090, accesat 30.10. 2021.

[57] Conform art. 12 alin. (1) din Directiva 2008/52/CE, termenul de transpunere a fost 21 mai 2011, cu excepția art. 10, pentru care asigurarea conformității trebuie să aibă loc cel mai târziu la 21 noiembrie 2010. Măsurile luate de către SM în vederea transpunerii Directivei 2008/52/CE, precum şi legislaţiile naţionale adoptate în acest scop sunt disponibile [Online] la https://eur-lex.europa.eu/legal-content/RO/NIM/?uri= CELEX:32008L0052, accesat 13.09.2021.

[58] C.T. Ungureanu, *Drept internațional privat european în raporturi de comerț internațional*, Editura Hamangiu, Bucureşti, 2021, p. 264.

[59] Pentru problematica legată de contractele electronice în dreptul comerțului internațional, a se vedea C.T. Ungureanu, *Dreptul comerțului internațional*, Editura Hamangiu, Bucureşti, 2018, pp. 155-192.

un act notarial sau hotărâre judecătorească şi dobândind valoarea unui titlu executoriu, acordul de mediere va putea fi pus în executare în SM conform prevederilor Regulamentului (UE) nr. 1215/2012, fără a fi necesară o hotărâre de încuviinţare a executării[60].

Deşi aprobarea acestui tratat multilateral de către UE ca organizaţie economică regională nu ar reprezenta o premieră, UE devenind anterior parte şi în alte convenţii internaţionale (*exempli gratia*, Convenţia de la Haga), acest moment nu pare a fi unul situat într-un viitor foarte apropiat. UE şi-a urmărit propria agendă în materia reglementării medierii în domeniul relaţiilor comerciale transfrontaliere, continuând procesul legislativ atât în timpul negocierilor purtate pentru elaborarea Convenţiei de la Singapore, cât şi după adoptarea acesteia. În UE au fost adoptate în perioada referită Regulamentul (UE) 2019/1150 al Parlamentului European şi al Consiliului din 20 iunie 2019 privind promovarea echităţii şi a transparenţei pentru întreprinderile utilizatoare de servicii de intermediere online[61] şi Directiva (UE) 2019/633 a Parlamentului European şi a Consiliului din 17 aprilie 2019 privind practicile comerciale neloiale dintre întreprinderi în cadrul lanţului de aprovizionare agricol şi alimentar[62].

O altă reglementare unională care prezintă importanţă din perspectiva rezervei pe care un stat sau organizaţiei regională poate să o formuleze în temeiul art. 8 alin. (1) din Convenţia de la Singapore este Acordul privind încetarea tratatelor bilaterale de investiţii dintre statele membre ale Uniunii Europene[63] care reglementează o formă *sui generis* de mediere între un investitor şi SM.

4. Motivele de refuz de recunoaştere a acordului de mediere

Cererea părţii interesate adresată autorităţii competente a unui stat parte la Convenţia de la Singapore pentru punerea în executare a acordului de mediere poate fi refuzată pentru motivele limitativ prevăzute la art. 5 din Convenţia de la Singapore.

Spre deosebire la prevederile Convenţiei de la New York în temeiul cărora nevaliditatea clauzei de arbitraj era prevăzută expres în textul tratatului ca reprezentând unul dintre motivele de refuz de executare a sentinţei arbitrale străine, aparent, Convenţia de la Singapore nu prevede acest motiv printre temeiurile refuzului punerii în executare a unui acord internaţional de mediere. Cu toate acestea, apreciem că lipsa validităţii formale a acordului de mediere poate fi încadrată motivului prevăzut de art. 5 alin. (1) lit. b) subpunctul i): acordul de

[60] Art. 58 și art. 59 din Regulamentul (UE) nr. 1215/2012.

[61] Publicat în JO L 186, 11.7.2019.

[62] Publicată în JO L 111, 25.4.2019; Pentru o analiză a medierii între profesioniști conform Regulamentului (UE) 2019/1150, a se vedea C.T. Ungureanu, *Drept internațional privat…*, *op. cit.*, pp. 266-270 .

[63] Publicat în JO L 169, 29.5.2020; Acordul a intrat în vigoare la 29 august 2020; Pentru o prezentare a acestei proceduri, a se vedea C.T. Ungureanu, *Drept internațional privat european…*, *op. cit.*, pp. 236-237.

soluţionare este caduc, inoperant sau nu este susceptibil de a fi pus în executare conform legii alese de către părţi sau în lipsa unei astfel de alegeri, în temeiul legii autorităţii competente a statului parte la convenţie în faţa căreia cererea a fost introdusă în temeiul art. 4 din Convenţia de la Singapore.

Termenii „caduc", „inoperant", „nesusceptibil de a fi aplicată" nu îşi regăsesc o definiţie în corpul Convenţiei de la Singapore. Autoritatea competentă chemată să se pronunţe asupra temeiniciei acestui motiv de refuz de punere în executare s-ar putea orienta spre explicaţiile pe care aceşti termeni le-au primit cu ocazia interpretării Convenţiei de la New York. În practică, s-a reţinut că excepţia caducităţii se referă la toate situaţiile în care convenţia este afectată de invaliditate încă de la încheierea sa[64], în timp ce o convenţie este inoperantă dacă a fost valabil încheiată dar şi-a încetat efectele[65] şi nu este susceptibilă de a fi aplicată în cazul în care nu se poate recurge la mijlocul alternativ de soluţionare a litigiului din cauza unor impedimente juridice sau fizice[66].

În această bază, partea căreia i se opune o cerere de executare a acordului de mediere ar putea invoca nevaliditatea formală a acordului de mediere încheiat prin mijloace electronice. Autoritatea competentă va trebui să stabilească mai întâi care este legea aplicabilă acordului internaţional de mediere şi apoi să cerceteze condiţiile pe care această reglementare le impune sub aspectul încheierii valide a unui acord de mediere. Dacă părţile au desemnat legea aplicabilă, autoritatea se va raporta la legea aleasă de către părţi. În sens contrar, legea aplicabilă va fi desemnată de autoritatea competentă urmând regulile stabilite în dreptul său intern.

Având în vedere similitudinea reglementărilor din Convenţia de la Singapore cu cele ale Convenţiei de la New York, răspunsul la întrebarea referitoare la stabilirea validităţii formale a acordului de mediere ar trebui urmeze aceleaşi principii şi soluţii judiciare exprimate cu privire la aplicarea art. 5 alin. (1) lit. a) din Convenţia de la New York[67].

Apreciem că, similar interpretării aplicării condiţiei validităţii impuse din Convenţia de la New York[68], acest motiv de refuz trebuie invocat de către partea căreia i se opune acordul de mediere şi nu de către autoritatea competentă din oficiu şi dovedit tot de către aceasta şi nu de către partea care solicită executarea.

[64] Consiliul international pentru arbitraj comercial, *Ghidul ICCA..., op. cit.,* p. 55.

[65] *Idem*, p. 56.

[66] *Ibidem.*

[67] UNCITRAL Secretariat *Guide on the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 1958)* 2016 Edition, pp. 151-152, [Online] la https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/2016_guide_on_the_convention.pdf, accesat 30.10.2021.

[68] *Ibidem.*

5. Concluzii

Viitorul soluţionării litigiilor de comerţ internaţional aparţine mijloacelor alternative de soluţionare a litigiilor, din care face parte şi medierea. Această tendinţă este una care s-a accentuat în ultimii ani. Istoria aplicării Convenţiei de la New York în ceea ce priveşte recunoaşterea şi executarea hotărârilor arbitrale străine îndreptăţeşte afirmaţia conform căreia succesul Convenţiei de la Singapore va depinde de numărul de state care vor înţelege să adere la această convenţie, de modalităţile concrete în care statelor vor integra în legislaţia naţională prevederile tratatului[69], precum şi de modul în care practicienii dreptului (avocaţi, mediatori) sau alte părţi interesate vor conştientiza beneficiile soluţionării litigiilor de comerţ internaţional prin mediere[70].

Totodată, impunerea medierii ca principal mijloc alternativ de soluţionare a litigiilor internaţionale este condiţionată de dezvoltarea unui infrastructuri juridice prin adoptarea unor reguli asupra procesului medierii, a codurile de conduită ale mediatorilor, dar şi de o viitoare jurisprudenţă care să ilustreze aplicarea în practică a Convenţiei[71].

Referinţe

Alexander N., Chong S., *UN Treaty on mediation signed in Singapore*, Nederlands-Vlaams tijdschrift voor mediation en conflictmanagement. 23, (2-3), 71-76, 2019 Singapore Management University School of Law Research Paper No. 14/2020, http://dx.doi.org/10.5553/tmd/138638782019023203008

Alexander N., Chong S., *Why is there no 'seat' of mediation?*, [Online]

Anderson D. Q., *The Singapore Convention on Mediation: Supplying the Missing Piece of the Puzzle for Dispute Resolution*, Forthcoming, Journal of the Malaysian Judiciary (Nov 2020), Singapore Management University School of Law Research Paper No. 1/2020, [Online]

Chong S., Steffek F., *Enforcement of International Settlement Agreement Resulting from mediation under the Singapore Convention – Private International Law Issues in Perspective*, Singapore Academy of Law Volume 31 (2019), [Online]

Chua E., *Enforcement of international mediated settlements without the Singapore convention on mediation*, (2019). Singapore Academy of Law Journal. 31, 572-597, Research Collection School Of Law, [Online]

Consiliul internaţional pentru arbitraj comercial, *Ghidul ICCA pentru interpretarea Convenţiei de la New York din 1958, Un ghid pentru Judecători*, [Online]

Franck S. D., *Challenges Facing Investment Disputes: Reconsidering Dispute Resolution în International Investment Agreements. Appeals mechanisms in international investment disputes*, Karl P. Sauvant, ed., Oxford University Press, 2008, Washington & Lee Legal Studies Paper No. 2009-03, [Online]

ICSID Arbitration Rules [Online]

[69] T. Schnabel, *Implementation of the Singapore Convention..., op. cit.*, pp. 277-289.

[70] T. Schnabel, *op. cit.*, p. 60.

[71] The Singapore International Dispute Resolution Academy, *A Handbook on the Singapore Convention on Mediation*, p. 25, [Online] la https://www.singaporeconvention.org/sites/singaporeconvention.org/files/SMU%20SOL%20Singapore%20Convention%20Mediation%20Handbook.pdf, accesat 12.09.2021.

Jura C., *O introducere în materia Convenției Națiunilor Unite privind Acordurile Internaționale Rezultate în urma Medierii - Convenția de la Singapore*, în Revista română de arbitraj nr. 1/2020, [Online]

Kessedjian C., *Droit du commerce international*, Ed. Presse Universitaires de France, Paris, 2013

McCormick K., Ong S.S. M., *Through the Looking Glass: An Insider's Perspective into the Making of Singapore Convention on Mediation* (2019) 31 Singapore Academy of Law Journal, [Online]

Morris-Sharma N. Y., *Constructing the Convention on Mediation: The Chairperson's Perspective* (2019) 31 Singapore Academy of Law Journal 487-519, [Online]

Salacuse J. W., *Is There a Better Way? Alternative Methods of Treaty-Based, Investor-State Dispute Resolution*, în Fordham International Law Journal, Volume 31, Issue 1 2007 Article 6, [Online]

Schnabel T., *The Singapore Convention on Mediation: A Framework for the Cross-Border Recognition and Enforcement of Mediated Settlements* (September 18, 2018). 19 Pepp. Disp. Resol. L.J. 1 (2019), http://dx.doi.org/10.2139/ssrn.3239527

Schnabel T., *Implementation of the Singapore Convention: Federalism, Self-Execution, and Private Law Treaties* (January 22, 2019). 30 Am. Rev. Int'l Arb., 265 (2020), p. 267, [Online]

SIDRA International Dispute Resolution Survey: 2020 Final Report, [Online]

Sîrbu M., *Metodele ADR în contextul european şi internaţional*, Editura Universul Juridic, Bucureşti, 2020

Steele B. L., *Enforcing International Commercial Mediation Agreements as Arbital Awards Under the New York Convention* în 54 UCLA Law Review 1385 (2007), pp. 1397-1399, [Online]

Sussman E., *The New York Convention Through a Mediation Prism*, în Dispute Resolution Magazine Volume 15, Number 4, Summer 2009, [Online]

The Singapore International Dispute Resolution Academy, *A Handbook on the Singapore Convention on Mediation*, [Online]

UNCITRAL Secretariat *Guide on the Convention on the Recognition and Enforcement of Foreign Arbitral Awards* (New York, 1958) 2016 Edition, https://doi.org/10.18356/661735a6-en

United Nations Conference On Trade And Development, *Investor-State Disputes: Prevention and Alternatives to Arbitration II*, United Nations New York and Geneva, 2011, [Online]

Ungureanu C.T., *Enforcement of the post- mediation agreement in international trade disputes*, în „Modernizarea legislaţiei naţionale în contextul uniformizării dreptului la nivel european şi implicaţiile socio-politice asupra sistemului administrativ", Editura Hamangiu, Bucureşti, 2014

Ungureanu C.T., *Dreptul comerţului internaţional*, Editura Hamangiu, Bucureşti, 2018

Ungureanu C.T., *Drept internaţional privat european în raporturi de comerţ internaţional*, Editura Hamangiu, Bucureşti, 2021

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-12

Buna-credinţă în contractele *click-wrap*

Good Faith in Click-Wrap Contracts

Sorin-Claude Modreanu[1]

Rezumat: Dreptul a avut dintotdeauna menirea de a răspunde necesităţilor societăţii, asigurând un cadru normativ raporturilor juridice desfăşurate în societate, care să imprime siguranţă circuitului civil. Evoluţia din ce în ce mai rapidă a tehnologiei reprezintă o provocare constantă pentru drept, care trebuie să-şi demonstreze capacitatea de adaptare şi să fie întotdeauna actual. Aşadar, într-o societate cu 4,9 miliarde de utilizatori internet (62% din întreaga populaţie) este firesc faptul că interacţiunile dintre drept şi internet sunt tot mai dese şi mai importante. În prezentul articol este analizat unul dintre cele mai utilizate contracte încheiate prin intermediul internetului, şi anume contractul de tip *click-wrap*, în care consimţământul este exprimat prin simpla apăsare a unei căsuţe. Astfel, este de interes modul în care funcţionează principiul general al bunei-credinţe din materia contractuală în astfel de acte juridice, ce efecte are acesta din urmă şi cum se aplică în această situaţie.
Cuvinte-cheie: internet; contracte de tip *click-wrap*; principiul bunei-credinţe; adaptare; efecte

Abstract: Law was always destined to answer all the necesities of society, making sure that there is a legal framework for the legal relationships which take place in society, that would induce certainity to the legal field. The ever faster technological evolution is a constant test for law, which has to demonstrate its capacity to adapt and always stay actual. Thus, in a society with 4.9 billions of internet users (62% of the entire population) it is only natural that interractions between law and internet are more frequent and important. In this article we analyze one of the most used remote contracts concluded through the internet, which is the click-wrap contract, in which the consent is expressed simply by clicking on an icon. Such, the way that the general contractual principle of good faith works in such legal acts, what are its effects and how it applies in this situation are of interest.
Keywords: internet; click-wrap contracts; the principle of good faith; adapt; effects

1. Introducere

Contractele sunt un motor indispensabil al evoluţiei noastre şi ne-au însoţit cu mult timp înainte să le cunoaştem relevanţa juridică în felul în care înţelegem

[1] Doctorand, Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iaşi, e-mail: modreanu.sorin@yahoo.com.

astăzi acest lucru. Astfel, contractele sunt parte din natura umană, deoarece omul este o ființă socială[2] și interacțiunea dintre oameni este un reflex.

Prin urmare, stadiul actual al dezvoltării economice a societății noastre se datorează abilității oamenilor de a elabora și de a încheia contracte. Felul, complexitatea și ingeniozitatea contractelor au reflectat întotdeauna stadiul tehnologiei existente, al resurselor disponibile și al capacității noastre de a le utiliza.

Structura contractuală actuală, ale cărei condiții fundamentale sunt, mai mult sau mai puțin identice de secole, este actualmente confruntată cu provocarea pe care o reprezintă internetul. Dintr-o societate de 7,9 miliarde de oameni[3], aproximativ 4,9 miliarde utilizează internetul[4] (62%), ceea ce înseamnă că interacțiunile dintre ramura juridică a contractelor și internet vor fi din ce în ce mai dese și mai intense.

În cuprinsul articolului vom încerca să stabilim dacă această nouă paradigmă a contractelor este în continuare compatibilă cu imemorialul principiu al bunei-credințe, care are o importanță deosebită în materia contractelor, dar care ar putea fi pus la îndoială în contextul contractelor de tip *click-wrap*.

2. Contracte (buna-credință în contracte)

Iată și motivul pentru care acest studiu prezintă relevanță. Deși imaginea pe care o avem când ne gândim la încheierea contractelor diferă enorm în funcție de perioada la care ne raportăm (tradițiunea în antichitate, o înțelegere verbală, o strângere de mână sau un alt gest ritualic, redactarea unui înscris sub semnătură privată, un click pe un ecran), principiul general al bunei-credințe, de această dată, privit în materia contractelor, le-a însoțit întotdeauna.

Întâi, într-o manieră foarte reducționistă, un contract reprezintă legea părților. Acestea consimt la anumite prestații, la modul în care vor fi executate și alte aspecte privitoare la raportul juridic pe care l-au creat în acest fel. Având în vedere caracterul esențialmente privat, în care părțile ajung singure la un acord care creează efecte juridice, este necesar, pe de o parte, să explicăm încrederea mutuală pe care și-o acordă părțile și pe de altă parte, un mecanism care să le protejeze de eventuale abuzuri.

Răspunsul la ambele întrebări este buna-credință. Doctrina definește în general buna-credință din două puncte de vedere, cel obiectiv și cel subiectiv[5]. Astfel, „ca stare psihologică a unui subiect de drept individual, se manifestă pe plan juridic, pe de o parte, sub forma intenției drepte, a diligenței, a liceității și abținerii de la producerea vreunui prejudiciu în executarea obligațiilor, în general, și a contractelor în special. Pe de altă parte, buna-credință îmbracă forma erorii

[2] Aristotel, *Politica*, Cartea I, Redactor Nicolae Năstase, Editura Antet, Oradea, 1996, p. 4.

[3] [Online] la https://www.worldometers.info/world-population/, accesat 26.10.2021.

[4] [Online] la https://datareportal.com/global-digital-overview, accesat 26.10.2021.

[5] S. Tisseyre, *Le rôle de la bonne foi en droit des contrats*, Essai d'analyse à la lumière du droit anglais et du droit européen, Editura Presses Universitaires d'Aix Marseille, Aix-en-Provence, 2012, p. 26.

scuzabile, adică a convingerii eronate şi neculpabile a unei persoane că are un drept şi că acţionează potrivit legii. În primul caz, *malitiis non est indulgendum*, legea sancţionează în diferite moduri reaua-credinţă ca act opus bunei-credinţe. În al doilea, eroarea scuzabilă, protejată ca atare de lege, echivalează cu un drept care înseamnă ocrotirea persoanei de bună-credinţă în contra consecinţelor iregularităţii unui act juridic"[6].

Aşadar, parte a principiului bunei-credinţe sunt comportamentul unei persoane care se circumscrie unor valori precum moralitatea, echitatea şi loialitatea, şi convingerea unei persoane că acţionează în mod just şi fără să prejudicieze interesele altuia, necunoscând aspectele care i-ar schimba această percepţie asupra situaţiei.

În cadrul prezentului studiu ne vom concentra atenţia asupra primei dimensiuni a acestui principiu, cea a bunei-credinţe obiective, aceasta fiind, în opinia noastră, relevantă din perspectiva compatibilităţii contractelor *click-wrap* cu principiul bunei-credinţe.

În dreptul român, principiul bunei-credinţe este afirmat întâi ca principiu general al ansamblului reglementării, situându-se în art. 14 C.civ.[7], iar mai apoi ca principiu contractual, în art. 1170 C.civ.[8] şi ca obligaţie în etapa negocierilor precontractuale, în art. 1183 C.civ.[9] Preocuparea legiuitorului pentru buna-credinţă, din momentul redactării noului Cod civil, este astfel evidentă.

Este necesar a lămuri câteva aspecte legate de conţinutul concret al acestei noţiuni. Astfel, s-a afirmat în doctrină că o prima obligaţie care se circumscrie principiului contractual al bunei-credinţe este cea de loialitate, care se traduce prin îndatorirea părţilor „de a se informa reciproc, adică de a prezenta toate datele şi elementele necesare pentru formarea în bune condiţii a contractului"[10]. La aceasta

---

[6] I. Deleanu, S. Deleanu, *Mică enciclopedie a dreptului*, Editura Dacia, Cluj-Napoca, 2000, p. 108-110 şi 210-211; D. Gherasim, *Buna-credinţă*, p. 34, 35, *apud* F.A. Baias, E. Chelaru, R. Constantinovici, I. Macovei (coordonatori), *Noul Cod civil, Comentariu pe articole*, ediţia a 2-a, Editura C.H. Beck, Bucureşti, 2014, p. 22.

[7] *„(1) Orice persoană fizică sau persoană juridică trebuie să își exercite drepturile și obligațiile cu bună-credință, în acord cu ordinea publică și bunele moravuri.*

(2) Buna-credință se prezumă până la proba contrară".

[8] *„Părțile trebuie să acționeze cu bună-credință atât la negocierea și încheierea contractului, cât și pe tot timpul executării sale. Ele nu pot înlătura sau limita această obligație".*

[9] *„(1) Părțile au libertatea inițierii, desfășurării și ruperii negocierilor și nu pot fi ținute răspunzătoare pentru eșecul acestora.*

(2) Partea care se angajează într-o negociere este ținută să respecte exigențele bunei-credințe. Părțile nu pot conveni limitarea sau excluderea acestei obligații.

(3) Este contrară exigențelor bunei-credințe, între altele, conduita părții care inițiază sau continuă negocieri fără intenția de a încheia contractul.

(4) Partea care inițiază, continuă sau rupe negocierile contrar bunei-credințe răspunde pentru prejudiciul cauzat celeilalte părți. Pentru stabilirea acestui prejudiciu se va ține seama de cheltuielile angajate în vederea negocierilor, de renunțarea de către cealaltă parte la alte oferte și de orice împrejurări asemănătoare".

[10] F.A. Baias, E. Chelaru, R. Constantinovici, I. Macovei (coordonatori), *op. cit.*, p. 1297.

s-ar adăuga, conform unei opinii, obligaţia de cooperare[11] a părţilor care înseamnă asigurarea unei echilibrări a prestaţiilor[12] şi conlucrarea acestora în sens de *ius fraternitatis*, în spiritul solidarităţii[13].

Cât despre conţinutul abstract al principiului bunei-credinţe, este mult mai larg şi într-o eternă schimbare, raportându-se la etică şi la morală, care evoluează concomitent cu societatea. În această dimensiune se circumscriu noţiuni precum corectitudine, solidaritate, deschidere şi mai ales încredere în „Celălalt"[14]. Ultima dintre noţiuni este indisolubil legată de spiritul contractului, şi anume de legătura privată dintre contractanţi. Părţile decid să dea naştere raportului juridic plecând de la prezumţia că cealaltă parte este sinceră, nu are alte intenţii decât cele menţionate şi convenite sau subînţelese şi că executarea contractului se va desfăşura în condiţii normale fără să fie nevoie de alte constrângeri pentru a determina partea să-şi respecte obligaţiile asumate. Aceasta este prezumţia relativă[15] de bună-credinţă, „*bona fides praesumitur*"[16], care ne salvează dintotdeauna de un formalism excesiv, cronofag şi nenatural (să fie oare aceste caracteristici negative puse sub semnul întrebării de apariţia aşa numitelor *smart contracts*[17]? [18]).

Iată deci o imagine generală şi mult simplificată a modului în care funcţionează principiul bunei-credinţe în materie contractuală.

3. Contractele click-wrap

Enunţăm faptul că, noile contracte *click-wrap* sunt contracte electronice şi contracte de adeziune.

În epoca internetului, s-a dezvoltat, în mod logic, o nouă tehnică de contractare[19], şi anume contractul electronic.

„Contractul electronic ar putea fi *definit* ca fiind contractul încheiat la distanţă, între absenţi, care, ca orice contract, presupune realizarea acordului de voinţe ale părţilor contractante, cu intenţia de a stabili, modifica sau de a stinge un

[11] I. Adam, A.R. Adam, *Codul civil. Cartea a V-a. Despre obligații, Titlurile I-VIII (art. 1164-1649)*, Comentarii și explicații, Editura C.H. Beck, București, 2016, p. 55.

[12] L. Pop, *Tratat de drept civil. Obligațiile,* volumul al II-lea, *Contractul*, Editura Universul juridic, București, 2009, p. 517, *apud* I. Adam, A.R. Adam, *op. cit.*, p. 55.

[13] *Ibidem.*

[14] V.M. Ciucă, *Bona fides într-o nouă hermeneutică*, în volumul Simpozionului „Disponibilități creative în lume", Societatea „Vasile Pogor", Iași, 2009, p. 14.

[15] I. Adam, A.R. Adam, *op. cit.*, p. 54.

[16] *Ibidem.*

[17] C.T. Ungureanu, *Drept internațional privat european în raporturi de comerț internațional*, Editura Hamangiu, București, 2021.

[18] I.-C. Leaua, prelegerea *Noile tehnologii și frontiere ale principiului legalității*, intervenție în cadrul Conferinței Naționale *Ipostaze ale principiului legalității în dreptul național și european*, 29.10.2021. S-a formulat opinia conform căreia în situația smart contracts, având în vedere modul în care operează acestea prin intermediul tehnologiei *blockchain*, prezumția este una de rea-credință, contrar modelului clasic.

[19] C.T. Ungureanu, *Contractul electronic*, Revista Dreptul, nr. 9, 2015, p. 159.

raport juridic concret, specific fiind modul de exprimare a acordului, în forma înscrisului electronic"[20]. Contractul electronic este reglementat în România prin două legi[21], şi anume Legea nr. 365/2002 din 7 iunie 2002, republicată, privind comerţul electronic[22] şi Legea nr. 455/2001 din 18 iulie 2001, republicată, privind semnătura electronică[23]. Prin urmare, noţiunea de înscris în formă electronică este definită în această din urmă lege, la art. 4, pct. 2, ca fiind *„o colecţie de date în formă electronică între care există relaţii logice şi funcţionale şi care redau litere, cifre sau orice alte caractere cu semnificaţie inteligibilă, destinate a fi citite prin intermediul unui program informatic sau al altui procedeu similar"*.

Conform alin. (1) al art. 7 din Legea nr. 365/2002 din 7 iunie 2002, republicată, privind comerţul electronic, contractelor încheiate prin mijloace electronice li se recunosc aceleaşi efecte precum contractelor obişnuite, *„atunci când sunt întrunite condiţiile cerute de lege pentru validitatea acestora"*. Conform alin. (3) al aceluiaşi articol, regimul probei încheierii unor astfel de contracte este supus dispoziţiilor Legii nr. 455/2001 din 18 iulie 2001, republicată, privind semnătura electronică. Art. 9 din Legea nr. 365/2002 din 7 iunie 2002, republicată, privind comerţul electronic prevede momentul încheierii contractului, stabilind la alin. (1) că acesta este cel al ajungerii acceptării ofertei de a contracta la cunoştinţa ofertantului. Alin. (2), însă, derogă de la regula generală în ceea ce priveşte momentul încheierii contractului, stabilind că în situaţia contractului *„care, prin natura sa ori la cererea beneficiarului, impune o executare imediată a prestației caracteristice se consideră încheiat în momentul în care debitorul acesteia a început executarea, în afară de cazul în care ofertantul a cerut ca în prealabil să i se comunice acceptarea. În acest ultim caz se aplică prevederile alin. (1)"*. Astfel se consacră teoria informaţiei, care derogă de la regula de drept comun pe care o reprezintă teoria recepţiei[24].

Observăm faptul că în principiu, derogările de la dreptul comun, reprezentat de actualul Cod civil, sunt punctuale şi nu afectează esenţa contractului (capacitate, consimţământ, obiect, cauză[25]), deci cel puţin sub aspectul definiţiei, există o similaritate între contractele electronice şi cele clasice[26].

Conform art. 1175 C.civ., contractul de adeziune este acea convenţie a cărei clauze *„esenţiale sunt impuse ori sunt redactate de una dintre părţi, pentru aceasta sau ca urmare a instrucţiunilor sale, cealaltă parte neavând decât să le accepte ca atare"*. Principalele caracteristici ale acestor contracte sunt inegalitatea economică a părţilor, caracterul general dar detaliat al ofertei şi atribuirea redactării clauzelor

[20] *Idem*, p. 162.

[21] *Idem*, p. 160.

[22] Publicat în M. Of. nr. 959 din 29 noiembrie 2006.

[23] Publicat în M. Of. nr. 316 din 30 aprilie 2014.

[24] C.T. Ungureanu, *Contractul electronic* ..., p. 173.

[25] L. Pop, I.-F. Popa, S.I. Vidu, *Drept civil. Obligațiile*, Ediția a II-a, revizuită și adăugită, Editura Universul Juridic, București, 2020, p. 56.

[26] D. Gărăiman, *De la contractul clasic la contractul electronic*, în *Codul civil român între tradiție și reformă la 140 de ani de aplicare*, în Revista Ştiinţe Juridice, 2006, p. 142, [Online] la https://drept.ucv.ro/RSJ/images/articole/2006/RSJ1/0119GaraimanD.pdf, accesat 29.10.2021.

esenţiale unei singure părţi[27]. Specificul unui contract ca fiind de adeziune atrage, atunci când un profesionist contractează cu un consumator, incidenţa legislaţiei în materie[28]. Astfel, „art. 4 alin. (1) din Legea nr. 193/2000 privind clauzele abuzive din contractele încheiate între profesionişti şi consumatori, republicată, prevede că o clauză abuzivă este acea clauză care nu a fost negociată direct cu consumatorul şi care, prin ea însăşi sau împreună cu alte prevederi din contract, creează, în detrimentul consumatorului şi contrar cerinţelor bunei-credinţe, un dezechilibru semnificativ între drepturile şi obligaţiile părţilor”[29].

Aceste noţiuni fiind explicate, ne vom apleca asupra contractelor *click-wrap*, care sunt, dintr-o subclasificare a contractelor electronice[30], „acele contracte de adeziune pentru încheierea cărora destinatarul unei oferte făcute online (pe Internet) trebuie doar să bifeze, într-o casetă (să facă un simplu *click* pe o pictogramă), butonul „Da”, „I accept”, „Yes” sau „I agree” ori altul similar şi contractul se perfectează”[31].

Având în vedere modalitatea specifică de exprimare a consimţământului, pot exista discuţii cu privire la validitatea unui consimţământ astfel exprimat. În acest sens, s-a afirmat în doctrină că „un gest neechivoc sau un comportament activ poate fi considerat ca o manifestare expresă a voinţei acceptantului. Pe de altă parte, pentru ca un contract să fie valabil format trebuie ca utilizatorul (acceptantul) să fie conştient că gestul său înseamnă admiterea efectivă a dispoziţiilor contractului de adeziune propus. Este motivul pentru care oferta trebuie să conţină toate datele particulare ale contractului”[32]. Aşadar, în materia contractelor *click-wrap*, depinde de iscusinţa (sau de buna-credinţă) a celor care redactează clauzele contractului pentru ca exprimarea consimţământului aderentului, în forma propusă de către cei dintâi, să producă efectele juridice prefigurate. Există suficiente metode la îndemâna celor care redactează contractul pentru a se asigura de acest lucru, iar cel mai important aspect este de a construi mecanismul în aşa fel încât să ofere anumite garanţii ale faptului că ansamblul dispoziţiilor contractuale a ajuns la cunoştinţa aderentului, fapt care poate fi realizat prin utilizarea unui limbaj explicit, prin plasarea pictogramei prin apăsarea căreia se manifestă acceptul aderentului la finalul documentului care conţine clauzele contractuale şi inclusiv prin plasarea întregului ansamblu de dispoziţii contractuale într-un singur loc.

Astfel, cum este situaţia majorităţii legislaţiilor, şi în România, din anul 2007, este recunoscută (de către ÎCCJ) exprimarea consimţământului prin contracte *click-wrap*[33]. Discuţiile şi nuanţările făcute în paragraful anterior rămân valabile, iar criteriile specifice urmează a fi decelate în doctrină şi în jurisprudenţă.

[27] I. Adam, A.R. Adam, *op. cit.*, p. 81.
[28] F.A. Baias, E. Chelaru, R. Constantinovici, I. Macovei (coordonatori), *op. cit.*, p. 1303.
[29] *Idem*, p. 1304.
[30] C.T. Ungureanu, *Contractul electronic* ..., pp. 164-165.
[31] *Idem*, p. 165.
[32] D. Gărăiman, *op. cit*, p. 148.
[33] C.T. Ungureanu, *Contractul electronic* ..., p. 174.

Spre exemplu, în doctrina din Statele Unite, s-a constatat că partea care a redactat contractul de adeziune (în acest exemplu, fiind vorba în special de contractele *online*) introduce deseori în contract clauze favorabile ei dar nerezonabile, mizând pe faptul că aderentul nu va citi contractul şi va da un consimţământ valabil pentru întregul contract[34].

4. Buna-credinţă în contractele click-wrap

Întrebarea pe care ne-o punem în acest context este dacă prevalenţa contractelor de tip *click-wrap* ne îndepărtează de principiul străvechi (dar uman şi necesar) al bunei-credinţe, sau dacă principiul este doar pliat în mod convenabil pe caracteristicile inedite (sau nu?) ale acestui tip de contract.

Astfel, pentru a răspunde la această întrebare, am încadrat contractul *click-wrap* în categoria contractelor electronice şi în specia contractelor de adeziune. În consecinţă, pentru trăsăturile pe care le împrumută de la aceste două apartenenţe, nu există motive ca principiul bunei-credinţe să fie pus la îndoială, în orice caz nu mai mult decât pentru situaţia separată a contractelor electronice şi a contractelor de adeziune în sine. Există însă anumite precizări care pot fi făcute.

În primul rând, „în prezent, părţile, într-o societate în care totul se desfăşoară cu viteză, nu se mai întâlnesc faţă în faţă, mai ales în cazul contractelor în care una dintre părţi este consumator”[35]. Contractele *click-wrap*, fiind contracte electronice, se încheie la distanţă, între absenţi. Aşa fiind, se poate pune problema, aşa cum a fost afirmat în doctrină, în legătură cu faptul că, în materie contractuală, „cunoaşterea identităţii cocontractantului este un element determinant al raporturilor contractuale pe care utilizatorul doreşte să le folosească”[36]. După cum am menţionat anterior, un aspect care ţine de principiul bunei-credinţe este acela al încrederii prezumate în cocontractant. Pentru a întări sentimentul de încredere, este important ca partea să-şi cunoască, atât cât este rezonabil posibil, cocontractantul. Este mult mai uşor pentru un om să se încreadă într-o figură pe care a văzut-o, decât în una pe care nu poate decât să şi-o imagineze. Deşi acesta este un aspect care poate fi întâlnit deseori în contractele între absenţi, în contractele *click-wrap* acesta va fi cazul mereu. Chiar şi în contractele pe care le încheie consumatorii cu profesioniştii, în care de multe ori aceştia nu iau contact decât cu un prepus al acestora din urmă, există o minimă interacţiune umană care poate fi de natură să stimuleze încrederea în aceştia. Deşi nu este un aspect determinant, este totuşi o limitare a înţelesului principiului bunei-credinţe. Se

[34] E.A. Zacks, *The restatement (Second) of contracts § 211 : Unfulfilled expectations and the future of modern standardized consumer contracts*, în Wayne State University Law School Legal Studies Research paper series no. 2016-14, pp. 736-738, [Online] la https://scholarship.law.wm.edu/wmblr/vol7/iss3/4/, accesat 26.10.2021.

[35] C.T. Ungureanu, *Implicațiile internetului în viața juridică*, în Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza” Iaşi, Tomul LXIII, Ştiinţe Juridice, 2017, nr. II, p. 2.

[36] D. Gărăiman, *op. cit.*, p. 143.

vorbeşte în doctrină despre „depersonalizarea, dematerializarea şi delocalizarea schimburilor prin internet”[37].

În al doilea rând, fiind în discuţie conţinutul concret al principiului bunei-credinţe, clauzele contractuale nu sunt şi nu pot fi negociate. Dacă am considera acest aspect ca fiind o atingere adusă principiului bunei-credinţe, atunci în orice caz nu ar fi una inedită, deoarece aceasta este situaţia contractelor de adeziune care sunt reglementate de mult timp şi şi-au păstrat acest caracter indiferent de modul în care a fost reglementat sau înţeles principiul bunei-credinţe. Aşadar, deşi acestea pot ridica anumite probleme în ceea ce priveşte buna-credinţă, neajunsurile sunt contrabalansate, cel puţin teoretic, de avantajele pe care le implică, precum rapiditatea întregii activităţi de contractare[38]. Într-o piaţă liberă şi extrem de dinamică, precum cea actuală, ar fi imposibil de imaginat ca fiecare contract încheiat pentru nevoi sau activităţi curente (mai ales pentru cele de o valoare economică redusă) să fie negociat. Ar fi o activitate extrem de cronofagă.

Spre exemplu, optica sistemului de *common law* din Statele Unite, exprimată prin *Restatement (Second) of Contracts*, desprinsă din prevederile Secţiunii 211 a fost aceea că o persoană care îşi exprimă consimţământul pentru un contract de adeziune pentru consumatori va fi ţinută de termenii contractuali chiar dacă aceasta nu i-a citit[39]. Însă chiar şi în această situaţie, buna-credinţă îşi găseşte aplicabilitatea, dar sub altă formă. Astfel, consumatorul va ţine cont de faptul că profesionistul încheie un contract similar cu un mare număr de persoane[40], şi „se va încrede în « buna-credinţă » a celui care a redactat contractul de adeziune”[41]. Trebuie precizat că în acelaşi articol din Secţiunea 211 din *Restatement (Second) of Contracts*, se menţionează şi faptul că atunci când profesionistul consideră că un consumator n-ar fi contractat dacă ar fi ştiut de existenţa unei anumite clauze, acea clauză nu va fi aplicabilă, completând în acest fel un oarecare echilibru între cele două părţi[42].

De asemenea, în contractele electronice, există o obligaţie de informare (art. 5 şi art. 8 din Legea nr. 365/2002 din 7 iunie 2002, republicată, privind comerţul electronic şi, pentru situaţia în care se contractează cu un consumator în calitatea acestuia de destinatar al serviciilor, O.U.G. nr. 34/2014, din 4 iunie 2014, privind drepturile consumatorilor în cadrul contractelor încheiate cu profesioniştii, precum şi pentru modificarea şi completarea unor acte normative[43]), sub sancţiunea nulităţii relative (art. 21 din Legea nr. 365/2002 din 7 iunie 2002, republicată, privind comerţul electronic)[44].

[37] *Idem*, p. 144.
[38] E.A. Zacks, *op. cit.*, p. 754.
[39] *Idem*, pp. 753-754.
[40] *Ibidem.*
[41] *Idem*, p. 754.
[42] *Idem*, pp. 755-756.
[43] Publicat în M. Of. nr. 427 din 11 iunie 2014.
[44] C.T. Ungureanu, *Contractul electronic ...*, p. 171.

Prin urmare, deşi există anumite limitări ale principiului bunei-credinţe în cazul contractelor de adeziune, deci inclusiv în cele *click-wrap*, ţinând cont de faptul că între acestea sunt contracte încheiate între profesionişti şi consumatori, o contrabalansare a limitărilor aduse efectelor principiului bunei-credinţe este cea dată de aplicabilitatea protecţiei speciale a consumatorilor (în dreptul naţional şi european). O altă limitare ar fi cea impusă de reglementarea clauzelor standard în contractele de adeziune[45].

5. Drept comparat sau compatibilitate cu internaţionalitatea contractelor de tip click-wrap

Având în vedere modul în care se încheie contractele de tip *click-wrap* şi circumstanţele specifice, în special faptul că cel care propune contractul de adeziune şi aderentul pot avea sediul respectiv domiciliul în state diferite, există o serie de precizări cu privire la legea aplicabilă contractului şi instanţa competentă să judece litigii izvorâte din contract[46]. Astfel, anumite state (cum sunt cele de *common law*, spre exemplu) înţeleg altfel principiul bunei-credinţe şi nu îl recunosc expres, ci doar indirect prin existenţa anumitor instituţii juridice cu efecte similare celor pe care le atribuie sistemele de drept continental în general principiului bunei-credinţe.

Deşi această ipoteză nu este singura posibilă, ne vom limita la a expune situaţia în ceea ce priveşte autoritatea competentă să soluţioneze un litigiu de drept internaţional privat izvorât dintr-un contract de tip *click-wrap* şi legea aplicabilă acestui raport juridic, când instanţa sesizată este cea română, autoritatea competentă să soluţioneze litigiul (prin convenţia validă a părţilor sau conform regulilor aplicabile) este o instanţă de judecată, iar părţile sunt un profesionist stabilit într-un stat membru al Uniunii Europene şi un consumator cu reşedinţa obişnuită în România, deoarece aceste calităţi ale părţilor şi particularităţi ale raportului juridic sunt foarte des întâlnite în litigiile izvorâte din contracte de tip *click-wrap*.

Aşadar, instanţa competentă poate fi aleasă prin „convenţia părţilor sau din prezentarea şi apărările pârâtului (prorogarea voluntară de competenţă)”[47] sau este stabilită conform normelor de competenţă aplicabile în temeiul legii forului[48].

Instanţa română sesizată cu un astfel de litigiu va proceda întâi la „determinarea instanţei competente de a soluţiona litigiul”[49]. În situaţia noastră, „Instanţa română are competenţă exclusivă în temeiul art. 1.080 C.pr.civ”[50]. Astfel, pct. 3 al art. 1.080 C.pr.civ. stabileşte că instanţa română este competentă pentru

[45] F.A. Baias, E. Chelaru, R. Constantinovici, I. Macovei (coordonatori), *op. cit.*, p. 1303.

[46] C.T. Ungureanu, *Contractul electronic ...*, p. 179.

[47] C. Dariescu, *Fundamentele dreptului internațional privat*, Ediția a V-a, revăzută și adăugită, Editura Universul Juridic, București, 2018, p. 56.

[48] C.-N. Bărbieru, C. Dariescu, *Fișe de drept internațional privat*, Colecția Examene, Editura Universul Juridic, București, 2020, pp. 52, 53, 56, 57, 62.

[49] C. Dariescu, *op. cit.*, p. 41.

[50] C.T. Ungureanu, *Contractul electronic ...*, p. 182.

„contracte încheiate cu consumatori având domiciliul sau reşedinţa obişnuită în România, pentru prestaţii de consum curent destinate uzului personal sau familial al consumatorului şi fără legătură cu activitatea profesională sau comercială a acestuia, dacă: a) furnizorul a primit comanda în România; b) încheierea contractului a fost precedată în România de o ofertă sau o publicitate şi consumatorul a îndeplinit actele necesare încheierii contractului". Astfel, „Competenţa exclusivă există atât pentru acţiunile introduse de consumator contra furnizorului cât şi invers"[51].

Având în vedere acest temei de competenţă exclusivă şi art. 1.068 alin. (2) C.pr.civ.[52], o eventuală convenţie de alegere a forului prin care părţile ar alege o altă instanţă decât cea română ca fiind competentă să judece litigiul în cazul unui contract *click-wrap* ar fi nulă[53], deoarece nesocoteşte un temei de competenţă exclusivă a instanţelor române[54].

Astfel, în ceea ce priveşte instanţa competentă, în ipoteza aleasă, întotdeauna va fi competentă instanţa română.

În ceea ce priveşte legea aplicabilă raportului juridic, există două ipoteze. Prima este cea în care se consideră că „regula *tării de origine* nu acoperă libertatea părţilor contractante de a alege legea aplicabilă contractului pe care l-au încheiat, care ar fi determinată potrivit normelor conflictuale din Roma I, nici obligaţiilor contractuale care privesc contracte încheiate cu consumatorii. Aceste obligaţii includ *informaţii cu privire la elementele esenţiale ale contractului, inclusiv drepturi ale consumatorilor, care au o influenţă determinantă asupra deciziei de a contracta*"[55]. Aşadar, acestor raporturi juridice li se aplică prevederile Regulamentului Roma I[56]. „Potrivit art. 6.1 Regulamentul Roma I, contractele încheiate între un consumator şi un profesionist sunt reglementate de legea statului în care îşi are *reşedinţa obişnuită consumatorul*, cu condiţia ca profesionistul să-şi desfăşoare activitatea comercială sau profesională în ţara în care îşi are reşedinţa obişnuită consumatorul,

[51] C. Dariescu, *op. cit.*, p. 56.

[52] *„Art. 1.068. Alegerea forului*

(1) În materie patrimonială, părţile pot conveni asupra instanţei competente să judece un litigiu actual sau eventual izvorând dintr-un raport cu elemente de extraneitate. Convenţia poate fi încheiată prin înscris, telegramă, telex, telecopiator sau orice alt mijloc de comunicare ce permite a-i stabili proba printr-un text. În lipsă de stipulaţie contrară, competenţa forului ales este exclusivă.

(2) Alegerea instanţei este fără efect dacă ea conduce la lipsirea în mod abuziv a uneia dintre părţi de protecţia pe care i-o asigură o instanţă prevăzută de legea română. De asemenea, alegerea este fără efect când instanţa aleasă este străină, iar litigiul este de competenţa exclusivă a instanţelor române, precum şi când instanţa aleasă este română, iar litigiul este de competenţa exclusivă a unei instanţe străine".

[53] C.T. Ungureanu, *Contractul electronic ...*, p. 183.

[54] C. Dariescu, *op. cit.*, pp. 57-58.

[55] A. Jaroszek, *European online marketplace – new measures for consumer protection against "old conflict of laws rules"*, în Masaryk University Journal of Law and Technology, 2015, p. 30; DOI: https://doi.org/10.5817/MUJLT2015-1-3.

[56] C.T. Ungureanu, *Drept internațional privat european în raporturi de comerț internațional...*, p. 98.

fie, prin orice mijloace, să-şi *direcţioneze* activităţile către ţara în cauză sau către mai multe ţări, printre care şi ţara în cauză, şi ca respectivul contract să se înscrie în sfera activităţilor respective"[57]. Dacă nu sunt îndeplinite condiţiile privind desfăşurarea activităţii în ţara în care îşi are reşedinţă obişnuită consumatorul, sau cele privind direcţionarea acesteia către ţara în care îşi are reşedinţa obişnuită consumatorul, se aplică prevederile art. 3 şi art. 4 ale Regulamentului Roma I[58]. De asemenea, în contractele încheiate între profesionişti şi consumatori este posibilă, în temeiul Regulamentul Roma I, o convenţie prin care părţile aleg legea aplicabilă contractului[59]. Astfel, „potrivit art. 6 alin. (2), alegerea de către părţi a legii aplicabile unui contract care îndeplineşte condiţiile specificate în art. 6 alin. (1), nu poate avea ca rezultat privarea consumatorului de protecţia pe care i-o asigură dispoziţiile imperative ale legii ţării în care consumatorul îşi are reşedinţa obişnuită"[60].

În a doua ipoteză, norma de drept internaţional privat din Legea nr. 365 din 7 iunie 2002, republicată, privind comerţul electronic[61], care stabileşte legea aplicabilă raporturilor juridice pe care le reglementează această lege, este considerată una de aplicaţie imediată[62]. Astfel cum reiese din dispoziţiile art. 3 al Legii nr. 365 din 7 iunie 2002, republicată, privind comerţul electronic, lege care, aşa cum se precizează în dispoziţiile finale ale acesteia, *„transpune Directiva 2000/31/CE referitoare la anumite aspecte juridice privind serviciile societăţii informaţionale, în special comerţul electronic în piaţa internă, publicată în Jurnalul Oficial al Comunităţilor Europene nr. L 178/2000"*, serviciilor societăţii informaţionale li se aplică legislaţia statului în care este stabilit furnizorul, dacă acesta este stabilit într-un stat membru al Uniunii Europene. Astfel, inclusiv în ipoteza în care părţile au încheiat o convenţie prin care aleg legea aplicabilă raportului juridic, aceasta va fi aplicabilă numai dacă coincide cu legea statului în care este stabilit furnizorul[63]. Interpretând aceste dispoziţii, cele ale alin. (40) al Preambulului Regulamentului (CE) nr. 593/2008 al Parlamentului European şi al Consiliului din 17 iunie 2008 privind legea aplicabilă obligaţiilor contractuale

[57] *Ibidem.*

[58] *Ibidem.*

[59] *Idem*, p. 99.

[60] *Ibidem.*

[61] *Art. 3. „Aplicarea legii române în cazul serviciilor societății informaționale. (1) Prezenta lege se aplică furnizorilor de servicii stabiliți în România și serviciilor oferite de aceștia. (2) De la data intrării în vigoare a prezentei legi serviciile societății informaționale sunt supuse: a) exclusiv prevederilor în vigoare ale legilor române care fac parte din legislația coordonată, în cazul în care sunt oferite de furnizori de servicii stabiliți în România; b) exclusiv prevederilor în vigoare ale legilor statului în cauză care fac parte din legislația coordonată, în cazul în care sunt oferite de furnizori de servicii stabiliți într-un stat membru al Uniunii Europene"*; publicată în M. Of. nr. 959 din 29 noiembrie 2006.

[62] C.T. Ungureanu, *Drept internațional privat european în raporturi de comerț internațional...*, p. 391.

[63] C.T. Ungureanu, *Contractul electronic ...*, pp. 180-181.

(Roma I)[64] şi cele ale art. 9 al aceluiaşi Regulament, în ceea ce priveşte legea aplicabilă contractelor încheiate prin mijloace electronice se aplică prevederile Legii 365 din 7 iunie 2002, republicată, privind comerţul electronic. Deci, în ipoteza noastră, a contractului *click-wrap*, legea aplicabilă contractului va fi cea a statului membru al Uniunii Europene în care este stabilit furnizorul de servicii.

Iată deci cum legea aplicabilă unui contract de tip *click-wrap* încheiat în condiţiile pe care le-am enunţat poate fi supus legii unor state diferite. Aşadar, întrebarea care se poate pune în contextul prezentului articol este dacă acest lucru aduce atingere în orice fel modului în care influenţează principiul contractual al bunei-credinţe contractul propriu-zis.

În majoritatea statelor membre ale Uniunii Europene[65], fiind sisteme de drept continental, principiul contractual al bunei-credinţe este cunoscut şi consacrat legislativ în forme asemănătoare. Aşadar, influenţa sa asupra unui astfel de contract este aceeaşi, indiferent de legea cărui stat european se va aplica.

În schimb, înaintea ieşirii Marii Britanii din Uniunea Europeană, era uşor de imaginat un contract *click-wrap* încheiat cu un consumator român căruia sa i se aplice legea Marii Britanii. Sistemele de *common-law*, dar mai ales cel britanic, nu recunosc existenţa unui principiu contractual al bunei-credinţe, întrucât contravine spiritului dreptului britanic aplecat către libertatea contractuală cvasi-absolută şi către diligenţa fiecărei părţi[66]. Această viziune este însă atenuată, cel puţin în privinţa efectelor, de instituţii care suplinesc necesitatea consacrării unui principiu general sau contractual al bunei-credinţe îndeplinind efectele acestuia. Aceste instituţii, ale căror efecte sunt asemănătoare celor pe care sistemele de drept continental le atribuie principiului bunei-credinţe, sunt *promissory estoppel*, *unjust enrichment*, *misrepresentation*[67] şi e*fficient breach of contract*[68]. Prin urmare, unui contract căruia i se aplică legea britanică, principiul contractual al bunei-credinţe din dreptul continental nu i se va aplica, dar va rămâne însă la adăpostul instituţiilor amintite.

[64] Publicat în Jurnalul Oficial al Uniunii Europene nr. L/177/6 în data de 4 iulie 2008.

[65] Spre exemplu, Codul civil francez, în art. 1104, astfel cum a fost modificat prin Ordonanța numărul 2016-131 din 10 februarie 2016, pentru reforma dreptului contractelor și a regimului general și al probei obligațiilor (traducerea ne aparține), publicat în M. Of. al Franței (*J. O.*) din 11 februarie 2016, reglementează principiul contractual al bunei-credințe. *„(1) Contractele trebuie negociate, încheiate și executate cu bună-credință. (2) Această dispoziție este de ordine publică”.*

[66] The Honorable Mr. Justice Steyn, *The Role of Good Faith and Fair Dealing in Contract Law: A Hair-Shirt Philosophy?*, The Royal Bank of Scotland Lecture, 1991, Oxford, published by arrangement with Mr. Justice Steyn and the Royal Bank of Scotland, p. 136.

[67] L. Péloquin, C. K. Assié, *Droit contractuel – La lettre d'intention*, în La Revue juridique Thémis (Québec), vol. 40, nr. 1/2016, pp. 192-193, *apud.* M. Floare, *op. cit.*, p. 224.

[68] *Idem*, p. 322.

6. Concluzii

Având în vedere cele prezentate în acest articol, considerăm că această nouă metodă de a contracta (contractele *click-wrap*) nu contravine principiului bunei-credinţe, datorită anumitor elemente care contrabalansează limitările punctuale aduse acestui principiu.

Conţinutul concret al principiului bunei-credinţe se păstrează, cu mici excepţii, care nu sunt însă suficiente pentru a pune sub semnul întrebării acest principiu contractual. Cât despre conţinutul abstract, şi anume despre încrederea dintre contractanţi, există anumite nuanţări, dar şi acestea sunt fireşti, având în vedere structura inedită (dacă privim întreaga istorie a contractelor) a acestui tip de contract.

Aşadar, nu se impune, din punctul nostru de vedere, o analiză atentă a eficacităţii principiului bunei-credinţe în acest nou context, deoarece, în prezent, nu există incompatibilităţi importante în coexistenţa acestuia cu modul în care funcţionează contractele *click-wrap*.

Referinţe

Adam I., Adam A.R., *Codul civil. Cartea a V-a. Despre obligaţii, Titlurile I-VIII (art. 1164-1649)*, Comentarii şi explicaţii, Editura C.H. Beck, Bucureşti, 2016

Aristotel, *Politica*, Cartea I, Redactor Nicolae Năstase, Editura Antet, Oradea, 1996

Baias F.A., Chelaru E., Constantinovici R., Macovei I. (coordonatori), *Noul Cod civil, Comentariu pe articole*, ediţia a 2a, Editura C.H. Beck, Bucureşti, 2014

Bărbieru C.-N., Dariescu C., *Fişe de drept internaţional privat*, Colecţia Examene, Editura Universul Juridic, Bucureşti, 2020

Ciucă V.M., *Bona fides într-o nouă hermeneutică*, în volumul Simpozionului „Disponibilităţi creative în lume", Societatea „Vasile Pogor", Iaşi, 2009

Dariescu C., *Fundamentele dreptului internaţional privat*, Ediţia a V-a, revăzută şi adăugită, Editura Universul Juridic, Bucureşti, 2018

Deleanu I., Deleanu S., *Mică enciclopedie a dreptului*, Editura Dacia, Cluj-Napoca, 2000

Gărăiman D., *De la contractul clasic la contractul electronic*, în *Codul civil român între tradiţie şi reformă la 140 de ani de aplicare*, în Revista Ştiinţe Juridice, 2006

Gherasim D., *Buna-credinţă*, p. 34, 35, *apud* Baias F.A., Chelaru E., Constantinovici R., Macovei I. (coordonatori), *Noul Cod civil, Comentariu pe articole*, ediţia a 2-a, Editura C.H. Beck, Bucureşti, 2014

Jaroszek A., *European online marketplace – new measures for consumer protection against „old conflict of laws rules"*, în Masaryk University Journal of Law and Technology, 2015; DOI https://doi.org/10.5817/MUJLT2015-1-3

Leaua I.-C., prelegerea *Noile tehnologii şi frontiere ale principiului legalităţii*, intervenţie în cadrul Conferinţei Naţionale *Ipostaze ale principiului legalităţii în dreptul naţional şi european*, 29.10.2021

Péloquin L., Assié C.K., *Droit contractuel – La lettre d'intention*, în La Revue juridique Thémis (Québec), vol. 40, nr. 1/2016, pp. 192-193, *apud* Floare M., *Buna şi reaua-credinţă în negocierea şi executarea contractelor de drept comun, în noul cod civil şi în dreptul comparat*, Editura Universul Juridic, Bucureşti, 2015

Pop L., Popa I.-F., Vidu S.I., *Drept civil. Obligaţiile*, Ediţia a II-a, revizuită şi adăugită, Editura Universul Juridic, Bucureşti, 2020

Pop L., *Tratat de drept civil. Obligaţiile,* volumul al II-lea, *Contractul*, Editura Universul juridic, Bucureşti, 2009

The Honorable Mr. Justice Steyn, *The Role of Good Faith and Fair Dealing in Contract Law: A Hair-Shirt Philosophy?*, The Royal Bank of Scotland Lecture, 1991, Oxford, published by arrangement with Mr Justice Steyn and the Royal Bank of Scotland

Tisseyre S., *Le rôle de la bonne foi en droit des contrats*, Essai d'analyse à la lumière du droit anglais et du droit européen, Editura Presses Universitaires d'Aix Marseille, Aix-en-Provence, 2012

Ungureanu C.T., *Contractul electronic*, Revista Dreptul, nr. 9, 2015

Ungureanu C.T., *Drept internaţional privat european în raporturi de comerţ internaţional*, Editura Hamangiu, Bucureşti, 2021

Ungureanu C.T., *Implicaţiile internetului în viaţa juridică*, în Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" Iaşi, Tomul LXIII, Ştiinţe Juridice, nr. II, 2017

Zacks E.A., *The restatement (Second) of contracts § 211 : Unfulfilled expectations and the future of modern standardized consumer contracts*, în Wayne State University Law School Legal Studies Research paper series no. 2016-14

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-13

Algoritmul – participant în procesul de încheiere a contractului

The Algorithm – Participant at the Conclusion of Contract

Crina-Maria Stanciu[1], **Codrin-Alexandru Ştefăniu**[2]

Rezumat: La momentul în care se doreşte încheierea unui contract, subiectul de drept se găseşte în ipostaza de a alege un scenariu potrivit acestei etape (fie negociază clauzele contractului, fie are loc un schimb al ofertei şi al acceptării). Cu toate acestea, insul urmăreşte adaptarea acestui proces la cerinţele din prezent pe care, de asemenea, omul şi nevoile schimbătoare le vor dicta (încheierea contractului într-un termen scurt; interpretarea corectă a clauzelor contractuale în vederea respectării voinţei reale a părţilor). În acest sens, lucrarea va încerca să releve nivelul de încredere pe care omul îl va putea avea în algoritm, pornind de la modul în care este acesta tratat din punct de vedere juridic, comparându-se condiţiile necesare a fi îndeplinite la încheierea unui contract cu modul în care este programat acest nou instrument.

Cuvinte-cheie: algoritm; contract; ofertă; acceptare; eroare

Abstract: At the moment when it is desired to conclude a contract, the subjects of law find themselves in the situation of choosing a scenario in accordance with this stage (either they negotiate the clauses of the contract or there is an exchange of offer and acceptance). However, the individual seeks to adapt this process to the current requirements that mankind and changing needs will also dictate (concluding the contract in a short time; correct interpretation of the contractual clauses in order to respect the real will of the parties). In this sense, the paper will try to reveal the level of trust that humans can have in the algorithm, starting from the way it is treated from a legal point of view, all the way to comparing the necessary conditions to be met when concluding a contract with how this new tool is program.

Keywords: algorithm; contract; offer; acceptance; error

1. Introducere

Lumea care ne înconjoară este una a schimbărilor generate de nevoile omului şi, ulterior, ale societăţii care îl cuprinde. Această „nevoie”, a cărui sens s-a lărgit din ce în ce mai mult, a determinat şi apariţia obligaţiei insului – mai întâi faţă de familie, ulterior faţă de persoanele din jur şi cu care intră în contact. Cu alte cuvinte,

[1] Doctorand, Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iași, e-mail: crinas17@yahoo.com.
[2] Teaching Assistant, University of Aberdeen Scotland, e-mail: codrinstefaniu36@gmail.com.

obligaţia a ajuns să lege omul de lucrurile din jurul său din ce în ce mai mult[3]. Astfel, insul sau subiectul de drept este legat prin uniune, percepută ca pe o formă a rudeniei – realizată prin intermediul căsătoriei[4]. De asemenea, se creează o convenţie prin intermediul legăturii de sânge care denotă încă o dată obligaţia pe care o avem unii faţă de ceilalţi în cadrul familiei. Familia poate fi, astfel, percepută drept izvorul unui prim contract pe care îl încheiem pe timpul vieţii.

Extrapolând sensul obligaţiei la nivelul societăţii, observăm creşterea numărului de înţelegeri care sunt realizate între oameni pentru urmărirea şi ducerea la bun final ale unor deziderate fie ele subiective sau obiective. Acestea din urmă sunt conduse spre punctul final prin intermediul unui schimb constant şi, respectiv, cu ajutorul mai multor îndatoriri pe care omul şi le asumă şi care se completează una pe cealaltă: a da, a primi şi a restitui[5]. La momentul în care încercăm să conturăm un raport obligaţional cu ajutorul acestora trei, ne gândim, înainte de toate, la formarea acestuia: la ofertă şi acceptare sau la parcursul negocierii. Ne punem întrebări precum aceea dacă putem sau nu constitui acel raport, ce formă va lua voinţa noastră în plan concret, dacă motivul realizării raportului obligaţional se încadrează în limitele prescrise de lege, respectiv, ce anume urmărim prin acel act. Toate aceste elemente vor fi discutate cu partea alături de care stabilim raportul obligaţional. Acest proces nu ar putea deveni, însă, mai simplu?

Omul a ajuns să evolueze din ce în ce mai mult: nevoile sale s-au schimbat, cerinţele s-au diversificat. A ajuns, în acest fel, la un impas: doreşte rezultatul finit al unei înţelegeri sau contract cât mai repede, iar acesta să se plieze voinţei şi solicitării sale. De aceea s-a creat un nou participant în procesul de formare al contractului părţilor, în ipostaza unui algoritm care să preia voinţa insului exprimată în plan abstract şi să o aducă în planul concret, gata de a fi implementată. Acestea, presupun, însă respectarea cuvântului dat, precum şi un schimb de consimţăminte, schimb pe care încercăm a-l realiza împreună cu un nou participant sau, chiar, o nouă formă de exprimare a consimţământului în plan juridic – algoritmul. Insul ajunge, astfel, să îşi exprime voinţa, dar mediat de un set de reguli care se pot schimba în funcţie de cerinţele imediate ale persoanei. Se realizează o convenţie a părţilor printr-un acord de voinţă care s-a dezvoltat pe baza a ceea ce a fost analizat şi interpretat prin cifre şi cuvinte.

2. Personalitatea juridică a algoritmului şi rolul acesteia în conceperea unui contract

Algoritmul reprezintă un proces ce conţine instrucţiuni, prin intermediul cărora un set de date de intrare se transformă într-un set de date de ieşire. Instrucţiunile au la bază calcule matematice ale căror caracteristici trebuie sa fie

[3] Gaius, *Instituțiunile*, trad. Aurel N. Popescu, Editura Academiei Republicii Socialiste România, Bucureşti, 1982, p. 218.

[4] A. Supiot, *Homo juridicus: eseu despre funcția antropologică a dreptului*, Editura Rosetti Educational, Bucureşti, 2011, pp. 150-151.

[5] *Idem*, p. 152.

suportate de un calculator. Datele de intrare şi cele de ieşire pot fi interpretate ca fiind modul de comunicare al unui algoritm cu lumea exterioară. Acesta transformă un şir de cifre binare într-un text care poate fi citit de către oameni. Numele „algoritm" a fost derivat din numele matematicianului Mohammed al-Khowârizmî care in secolul al IX-lea a creat regulile pentru adunări, scăderi, înmulţiri şi împărţiri ale numerelor raţionale[6]. Numele acestuia, a fost tradus iniţial în latină sub forma „*Algorismus*", din care a derivat versiunea actuală a cuvântului „algoritm"[7]. Primul algoritm a fost inventat de către matematicianul grec Euclid, în jurul anului 300 î.Hr[8]. Acest algoritm are funcţionalitatea de a găsi cel mai mare divizor comun a două numere[9].

În continuare ne dorim să prefigurăm modul în care algoritmul ar pute fi inclus în sfera juridică. Cu alte cuvinte, vom încerca să integrăm algoritmul în rândul subiectelor de drept capabile a se obliga şi a-şi exercita drepturile. Astfel, prin interpretarea art. 2 alin. (1) C. civ. *Dispoziţiile prezentului cod reglementează raporturile patrimoniale şi nepatrimoniale dintre persoane, ca subiecte de drept civil.* coroborat cu art. 25 alin. (2) şi (3) C. civ. *Persoana fizică este omul, privit individual, ca titular de drepturi şi de obligaţii civile. Persoana juridică este orice formă de organizare care, întrunind condiţiile cerute de lege, este titulară de drepturi şi de obligaţii civile.* ni se arată că, pentru a fi considerat subiect de drept în sensul legii civile, este necesară calitatea de om, de persoană care evoluează odată cu societatea în care trăieşte, ori calitatea de subiect colectiv, care îndeplineşte condiţiile cerute de lege. Prin urmare, definitoriu pentru sfera legală a unei societăţi este modul în care a ales legislaţia să trateze noţiunea de „persoană", aşa cum o arăta şi filozoful Gustav Radbruch[10]. În dreptul roman, lexemul „persoană" sau *persona* era utilizat pentru a ilustra diferitele roluri pe care le avea omul în variatele momente ale vieţii sale. Astfel, acesta putea deţine o varietate de *personae* – *pater familias,* angajator, membru de familie, vânzător, testator[11]. Aceste roluri creau imaginea statutului pe care omul îl ocupa în societatea romană – fie prin analiza lui *status libertatis* (oameni liberi şi sclavi), *status civitatis* (diferenţia cetăţenii de străini) şi *status familiae* (*paterfamilias* sau *filiusfamilias*). Ceea ce poate fi remarcat este inexistenţa legăturii dintre *persona* şi omul în sens biologic – *persona* aducea cu sine statutul, rolul legal, capacitatea legală, iar omul în sens biologic aducea doar carcasa care urma a fi umplută sau nu de viaţă juridică.

---

[6] H. Gabriel, *Secretele Algoritmului*, p. 2, [Online] la https://sites.google.com/site/secretelealgoritmului/ce-este-un-algoritm, accesat 12.10.2021.

[7] *Ibidem.*

[8] *Idem,* p. 3

[9] *Ibidem.*

[10] B. van Beers, *The Changing Nature of Law's Natural Person: The Impact of Emerging Technologies on the Legal Concept of the Person*, în *German Law Journal*, Vol. 18, No. 03, p. 560, [Online] la https://www.researchgate.net/publication/331613123_The_Changing_Nature_of_Law's_Natural_Person_The_Impact_of_Emerging_Technologies_on_the_Legal_Concept_of_the_Person, accesat 12.09.2021.

[11] *Idem,* p. 572.

În continuare, vom încerca să aflăm dacă *persona* sau conţinutul juridic al subiectului de drept nu ar putea fi conferit şi unui algoritm, la momentul în care acesta este inclus în cadrul procesului de formare al unui contract. Astfel, trebuie, în primul rând avut în vedere faptul că acordarea personalităţii juridice unei noi entităţi presupune crearea unei ficţiuni juridice capabile să se adapteze cerinţelor prezentului. Algoritmul reprezintă nevoia de adaptare a societăţii la planul economic, juridic, social care s-a creat prin evoluţia tehnologică[12]. Urmare a acestui fapt, vom încerca prefigurarea unei forme juridice care să explice şi să constituie un cadru legislativ potrivit utilizării algoritmului în materie precontractuală. Am putea încadra, în primul rând, algoritmul în sfera persoanelor fizice?

Pentru a realiza acestea ar trebui ca algoritmul să facă parte din specia umană; personalitatea acestuia să îşi găsească începutul în naştere, iar moartea să reprezinte punctul final al demersului nostru[13]. Algoritmul, spre deosebire de om, nu se naşte sau moare, ci este construit şi ar putea, cândva, să prezinte erori de funcţionare[14]. De asemenea, algoritmul nu presupune o organizare de sine stătătoare şi un patrimoniu aparte, spre a putea fi considerat o persoană juridică. Cu toate acestea, prezintă un scop bine determinat prin prisma regulilor pentru care este construit. Astfel, putem observa un transfer incipient de cunoştinţe aferente omului, privit individual, către algoritm, privit ca pe un intermediar pentru ceea ce doreşte a realiza insul. Omul se schimbă, iar această schimbare determină modificarea mediului legislativ prin crearea unui nou participant în materie contractuală, pe care îl vom numi în continuare agent al voinţei insului sau intermediar între voinţa unei persoane şi voinţa altei persoane.

Algoritmul, agentul sau intermediarul dintre voinţa unei persoane şi a alteia, ar putea fi analizat şi conceput fie ca pe o persoană juridică cu drepturi recunoscute de lege, fie drept un spaţiu care să adăpostească capacitatea persoanei şi care să dobândească, în acest fel, drepturi, fie ca pe un spaţiu care acumulează o aptitudine sau capacitate în vederea creării unor relaţii legale[15]. Care ar fi soluţia cea mai potrivită?

3. Formarea contractului şi rolul acordat algoritmului în cadrul acestui proces

Care este fundamentul în virtutea căruia sunt negociate şi acceptate variatele oferte ale cocontractanţilor prin intermediul inteligenţei artificiale? Cu alte cuvinte, inteligenţa artificială va acţiona în acest demers drept un reprezentant

[12] R.F. Reier Forradellas, *Digital Transformation and Artificial Intelligence Applied to Business: Legal Regulations, Economic Impact and Perspective*, în *Laws*, 2021, pp. 1-3, [Online] la https://www.mdpi.com/2075-471X/10/3/70/html, accesat 10.10.2021.

[13] B. van Beers, *op. cit.*, p. 563.

[14] M.D. Bob, *Manual elementar de drept privat roman*, Editura Universul Juridic, Bucureşti, 2019, p. 87.

[15] J.C. Gellers, *Rights for Robots. Artificial Intelligence, Animal and Environmental Law*, Editura Routledge, New York, 2021.

legal al uneia dintre părţi faţă de cealaltă sau aceasta nu poate fi percepută decât ca pe un simplu instrument al cocontractantului[16]? În ambele ipoteze prezentate se remarcă un principal factor de risc în realizarea contractului, respectiv, dacă algoritmul, la momentul în care va negocia clauzele actului pentru partea care îl utilizează, exprimă sau nu un consimţământ valabil. Astfel, în continuare vor fi ilustrate două modalităţi de organizare a procesului de încheiere a contractului, pornindu-se de la scenariul care trebuie urmat, ca regulă, în această materie.

În primul rând, pentru încheierea unui contract va fi necesară exteriorizarea consimţământului părţilor în sensul intenţiei de a fi legate de termenii şi de condiţiile asupra cărora acestea au convenit. În acest fel, ne sunt devoalate şi condiţiile de validitate care trebuie, de asemenea, îndeplinite de contractanţi pentru ca actul respectiv să îşi producă efectele sub auspiciile libertăţii de voinţă a părţilor: capacitate, consimţământ, obiect şi cauză a actului juridic[17].

În ceea ce priveşte condiţia capacităţii, respectiv – a aptitudinii părţilor de a fi titulare de drepturi şi de obligaţii aduse împreună cu ajutorul contractului – vom încerca a prefigura un transfer de capacitate dinspre persoana interesată spre algoritm, astfel încât acesta să poată încheia acel act, deoarece partea pentru care a intervenit are capacitatea necesară[18]. Acestea se vor petrece la momentul la care utilizăm un algoritm pentru negocierea clauzelor unui contract.

Obiectul şi cauza contractului trebuie să existe, să fie bine determinate, posibile şi să fie în acord cu legea şi cu morala. Cele două condiţii de validitate ale contractului menţionate anterior vor putea fi identificate prin intermediul termenilor şi condiţiilor actului, astfel încât să reflecte ceea ce au urmărit părţile a realiza în plan juridic. În ceea ce priveşte algoritmul în contracte, condiţiile vor putea fi determinate prin raportare la setul de date, de reguli care i-au fost atribuite algoritmului, date care reflectă, de fapt, voinţa finală a părţilor.

În ceea ce priveşte consimţământul părţilor, respectiv manifestarea de voinţă în sensul încheierii unui contract, vom avea în vedere, pe de o parte, parcursul intern de formare a consimţământului, acesta din urmă trebuind a fi serios, liber şi exprimat în cunoştinţă de cauză, punându-se un mare accent pe existenţa sau pe inexistenţa viciilor de consimţământ[19]. În cadrul parcursului extern care ilustrează în realitate, în planul concret, voinţa părţilor, consimţământul poate fi conturat fie prin negocierea contractului, fie prin aducerea laolaltă a ofertei şi a acceptării[20].

---

[16] M. Oliver, *Contracting by artificial intelligence: open offers, unilateral mistakes, and why algorithms are not agents*, în *Australian National University Journal of Law and Technology*, 2021, p. 47, [Online] la https://anujolt.org/article/24466-contracting-by-artificial-intelligence-open-offers-unilateral-mistakes-and-why-algorithms-are-not-agents, accesat 18.10.2021.

[17] C.T. Ungureanu, *Drept civil. Partea generală. Persoanele*, Editura Hamangiu, Bucureşti, 2013, p. 127.

[18] *Idem*, p. 128.

[19] *Idem*, pp. 127-128.

[20] L. Pop, I.-F. Popa, S.I. Vidu, *Curs de drept civil. Obligațiile*, Editura Universul Juridic, București, 2015, p. 53.

Consimţământul este o condiţie aparte şi care nu poate fi uşor îndeplinită prin intermediul algoritmului. Această exteriorizare a consimţământului presupune scoaterea la liman a intenţiei, a voinţei de a contracta a părţilor. Pe de o parte, ne gândim la realizarea negocierilor prin încheierea unor acte care să poată ilustra mai bine această voinţă; dar, din nou, ne punem întrebarea cum ar putea algoritmul să exprime voinţa părţii pentru care intervine la nivelul unei scrisori de intenţie, unui pact de opţiune sau a unei promisiuni de a contracta. Mai mult decât atât, cum va putea realiza algoritmul acestea în cadrul mecanismului de formare a contractului prin constituirea unei oferte şi acceptarea acesteia. Observăm, de asemenea, necesitatea îndeplinirii condiţiilor de validitate anterior menţionate inclusiv în ceea ce priveşte aceste acte (oferta fiind un act juridic unilateral prin care se propune unei alte părţi încheierea unui contract în anumite condiţii, conform art. 1.188 alin. (1) C. civ., iar acceptarea fiind actul prin intermediul căruia voinţa este redată în sensul achiesării la încheierea contractului în anumite condiţii[21]).

În sistemul de drept anglo-american, este schimbată definiţia contractului, acesta reprezentând o sumă de promisiuni care vor conduce la încheierea şi executarea acestuia[22]. Astfel, aducem împreună mai multe promisiuni care vor crea sfera de aplicare a contractului. De asemenea, promisiunea presupune aducerea în prim-plan a elementelor circumscrise voinţei, precum şi intenţia subiectului de drept de a respecta cele la care s-a obligat[23]. Astfel, oferta şi acceptarea vor putea fi înţelese drept promisiuni legate printr-o condiţie – promisiunea de a face, a nu face sau a da ceva, în schimbul promiterii contraprestaţiei de către cealaltă parte[24]. Se vorbeşte, în acest fel, despre existenţa unei condiţii suspensive – cealaltă parte trebuie, de asemenea, să realizeze o promisiune, pentru a putea fi creat actul juridic în cauză. Mai mult decât atât, prin acest schimb de promisiuni se ajunge la îndeplinirea lui *consideration*[25] (sau beneficiul urmărit prin încheierea contractului), asemuit cauzei sistemului de drept din România. Aceste promisiuni, de asemenea, vor prezenta manifestarea de voinţă a unei persoane, iar algoritmul va avea sau nu un rol important în acest demers, chiar de participant indirect. Ceea ce importă este voinţa ofertantului (intenţia ca oferta să fie acceptată de cealaltă

[21] *Idem*, p. 80.

[22] Restatement Second of Contracts § 1. *"A contract is a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty".*

[23] La nivelul Europei, se remarcă un interes crescut pentru modul în care se formează contractul și, mai cu seamă, în articolul 2:101 din cadrul *The Principles of European Contract Law: "A contract is concluded if: the parties intent to be legally bound, and they reach a sufficient agreement without any further requirement".*

[24] M. Hogg, *Promises and Contract Law. Comparative Perspectives,* Editura Cambridge University Press, The Edinburgh Building, Cambridge, 2011, p. 210.

[25] E.W. Weitzenböck, *English Law of Contract: Consideration*, în *Norwegian Research Center for Computers & Law*, 2012, p. 2, [Online] la https://www.uio.no/studier/emner/jus/jus/JUS5260/v12/undervisningsmateriale/Consideration.pdf, accesat 18.10.2021.

parte), dar şi caracterul cert, respectiv; comunicarea ofertei către posibilul cocontractant[26].

Pentru a putea înţelege mai bine rolul algoritmului în cadrul procesului de formare a contractului, au fost create două teorii care au aplicabilitate atât la nivelul negocierilor, cât şi la nivelul mecanismului de ofertă şi acceptare[27]. Aceste teorii gravitează în jurul sistemului de drept anglo-american, dar; după cum se va putea observa, acestea vor putea să îşi găsească aplicarea şi în sfera dreptului român.

În primul rând, s-a argumentat în sensul utilizării algoritmului drept reprezentant al părţii pentru care intervine şi negociază sau acceptă ori realizează o ofertă[28]. Teoria reprezentării juridice aduce cu sine, astfel, posibilitatea de negociere şi de încheiere a contractului prin transferarea unei părţi a autorităţii subiectului de drept către algoritm, respectiv; voinţa persoanei se va putea realiza prin intermediul acestuia. Condiţia de validitate a consimţământului va fi, prin urmare, respectată. Se consideră, însă, că interesul părţii este alterat de intervenţia algoritmului, deoarece acesta va constitui oferta cu ajutorul unui *input* general. De asemenea, reprezentantulva fi unul artificial deoarece acesta nu este o persoană, „om, privit individual"[29]. S-a creat, astfel, o ficţiune juridică pentru a acoperi o lacună în domeniu. Totodată, legea va trebui să se reorienteze şi să considere intenţia şi cunoştinţele incluse în algoritm la fel cum ar trata raportul dintre reprezentat şi reprezentant (cunoştinţele reprezentantului sunt ale reprezentatului). În plus, algoritmul nu va mai trebui inclus în sfera subiectelor de drept, a persoanelor, putând să îşi realizeze scopul fără a mai fi necesară acordarea unor drepturi şi obligaţii distincte. Mai mult decât atât, *Uniform Electronic Transactions Act* (1999) prezintă o formulare din care putem deduce susţinerea acestei teze prin faptul că încearcă facilitarea încheierii de contracte prin intermediul algoritmilor, cu ajutorul unor dosare electronice sau evidenţe electronice şi a semnăturii electronice (se creează o egalitate între dosarul fizic, semnătura olografă şi

[26] G. Quinot, *Offer, Acceptance, and the Moment of Contract Formation*, *in loc. cit.*, Hector MacQueen, Reinhard Zimmermann, *European Contract Law. Scots and South African Perspectives*, Editura Edinburgh University Press, Edinburgh, 2006, pp. 76-78.

[27] Aceste teorii au trebuit a fi formulate și datorită lacunelor legislative în materie de contracte, precum și al modului în care percep teoreticienii și practicienii dreptului schimbarea tehnologică care planează în această sferă (algoritmul va realiza sarcini complexe; algoritmul va putea fi perceput fie ca pe o mașinărie, fie ca pe un agent/reprezentant al părții; noile reguli care vor fi impuse în ceea ce privește reponsabilitatea algoritmului în cazul în care nu se respectă cele prezentate în momentul negocierii și al stabilirii clauzelor contractuale). U. Pagallo, *The Laws of Robots: Crimes, Contracts, Torts*, Editura Springer Science+Business Media Dordrecht, Dordrecht Heidelberg New York London, 2013, p. 94.

[28] L.H. Scholz, *Algorithmic Contracts*, în *Stan. Tech. L. Rev.*, nr. 128, Stanford, California, 2017, p. 164, [Online] la https://law.stanford.edu/publications/algorithmic-contracts/, accesat 1.10.2021.

[29] S. Chopra, L.F. White, *Artificial Agents and the Contracting Problem: A Solution Via an Agency Analysis*, în *University of Illinois Journal of Law Technology & Policy*, 2010, pp. 363-365, [Online] la https://ssrn.com/abstract=1589564, accesat 15.10.2021.

instrumentele electronice)[30]. Algoritmul va putea, prin urmare, să semneze contractul, iar rezultatul negocierilor va putea fi inclus într-un registru electronic (putându-se proba cele realizate de algoritm). Raportul dintre reprezentat şi reprezentant se va contura fie prin convenţie, fie prin ratificare, cea de pe urmă metodă fiind aceea care să fie utilizată pentru a lega partea de cel care va acţiona în interesul ei. Ratificarea va fi folosită deoarece societăţile/persoanele juridice şi persoanele nu vor putea să prevadă fiecare acţiune a algoritmului, dar prin ratificare procedeul se simplifică. Se pot crea modalităţi de evaluare a algoritmului în actele pe care le încheie, iar reprezentantul va avea, în acest fel, control asupra activităţii algoritmului[31]. Cu alte cuvinte, la momentul în care algoritmul va încheia un contract, cel reprezentat va avea posibilitatea de a-l analiza, iar în cazul în care actul respectiv nu ar fi considerat a fi încheiat în interesul său, persoana va avea posibilitatea de a refuza ratificarea acelui act. Cu toate acestea, va exista un risc pe care reprezentatul să şi-l asume pentru cazul în care algoritmul nu va funcţiona corespunzător sau nu va executa contractul format în conformitate cu cerinţele negociate.

O a doua teorie care încearcă a o înlocui pe cea precedentă a fost formulată de Matthew Oliver. Acesta consideră că teoria reprezentării nu permite respectarea regulilor aplicabile actualmente în contracte[32]. Cu alte cuvinte, se propune o teorie aplicabilă în cadrul legislaţiei în vigoare şi a teoriilor existente, fără a fi necesară modificarea acestora din urmă. Astfel, algoritmul va fi tratat ca pe o maşinărie, ca pe un instrument al omului, al subiectului de drept, menit să eficientizeze negocierea contractului ori schimbul ofertă/acceptare. Pentru sprijinirea acestei opinii se aduce în prim-plan cauza *Quoine Pte Ltd v B2C2 Ltd* adusă în faţa Curţii de Apel din Singapore pe data de 24 februarie 2020. Aceasta descrie problema validităţii comerţului şi investiţiilor realizate cu ajutorul Bitcoin şi Etherum. Astfel, Quoine a creat un program prin care a instituit o piaţă de tranzacţionare a Bitcoin şi Etherum. Un algoritm era folosit pentru a negocia şi a încheia contractele avute în vedere. Ca urmare a unei probleme tehnice, algoritmul nu a mai putut accesa datele referitoare la preţurile curente. Partea adeversă, denumită în continuare B2C2, dorind să cumpere Bitcoin, a utilizat preţul său de rezervă, stabilit pentru

[30] *"(6) "Electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual. (7) "Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means. (8) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.",* [Online] la https://www.uniformlaws.org/ committees/community-home? CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034, accesat 1.10.2021.

[31] L.H. Scholz, *op. cit.*, pp. 165-167.

[32] M. Oliver, *Contracting by artificial intelligence: open offers, unilateral mistakes, and why algorithms are not agents*, în *ANU Journal of Law and Technology*, Vol. 2, 2021, p. 74, [Online] la https://anujolt.org/article/24466-contracting-by-artificial-intelligence-open-offers-unilateral-mistakes-and-why-algorithms-are-not-agents, accesat 10.10.2021.

cazul în care ar apărea o situaţie neprevăzută, oferind la schimb Etherum. Preţul Bitcoin a scăzut, determinând mai mulţi investitori să vândă Bitcoin la cel mai bun preţ arătat de platformă până la acel moment, preţ care coincidea cu acela de rezervă al B2C2. În acest fel, B2C2 a cumpărat milione de dolari (tranzacţionaţi în Bitcoin) la o rată de 250 de ori mai bună decât rata stabilită pe piaţă. Aceste proceduri nu au putut fi observate imediat, fiind realizate prin intermediul algoritmilor. Ulterior, Quoine a anulat tranzacţiile, considerându-le greşeli. B2C2, însă a acţionat în justiţie Quoine considerând tranzacţiile realizate contracte definitive şi care obligă părţile[33].

În baza legii din Singapore, un contract poate fi desfiinţat pentru eroare unilaterală dacă partea care nu se afla în eroare avea cunoştinţă despre această eroare[34]. Quoine s-a folosit de acestea şi, calificând algoritmul drept reprezentant al său, a susţinut în continuare anularea contractelor încheiate sub imperiul unei greşeli sau erori. În plus, algoritmul care a cumpărat pentru B2C2 avea toate cunoştinţele necesare pentru a remarca inclusiv greşeala comisă pe piaţa virtuală. În acest fel, Quoine a arătat că actele juridice au fost încheiate între vânzători şi cumpărători, prin reprezentare. Cu toate acestea, Curtea a stabilit că algoritmul este un instrument, fără raţiune, iar cunoştinţele la care legislaţia se referă sunt acelea ale programatorului, programator care nu cunoştea ivirea defecţiunii[35]. Quoine este principalul actor, aflat în mijlocul a numeroase contracte, toate raporturile realizându-se prin intermediul platformei, care funcţiona şi dirija oferta şi acceptarea părţilor. În acest fel se formau numeroase contracte, dar la baza acestora se aflau termenii din ofertă, alături de acceptare (sau contraofertă-acceptare). Soluţia pe care a acceptat-o Curtea a fost aceea de a da efect teoriei contractuale, fundamentându-şi argumentele pe schimbul dintre ofertă şi de acceptare[36].

---

[33] L.B.M.R. Hakim, *Do Algorithms Dream of Mistaken Contracts? Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 2*, [Online] la https://smulexicon.com/2020/05/15/do-algorithms-dream-of-mistaken-contracts-quoine-pte-ltd-v-b2c2-ltd-2020-sgcai-2/, accesat 2.10.2021.

[34] M. Oliver, *op. cit.*, pp. 75-76.

[35] Quoine Pte Ltd v B2C2 Ltd, Court of Appeal of the Republic of Singapore, în *Civil Appeal No. 81*, 2019.

"Where it is relevant to determine what the intention or knowledge was underlying the mode of operation of a particular machine, it is logical to have regard to the knowledge or intention of the operator or controller of the machine. In the case of the kitchen blender, this will be the person who put the ingredients in and caused it to work. His or her knowledge or intention will be contemporaneous with the operation of the machine. But in the case of robots or trading software in computers this will not be the case. The knowledge or intention cannot be that of the person who turns it on, it must be that of the person who was responsible for causing it to work in the way it did, in other words, the programmer.", [Online] la https://www.sicc.gov.sg/docs/default-source/modules-document/judgments/quoine-pte-ltd-v-b2c2-ltd.pdf-, accesat 20.10.2021.

[36] M. Oliver, *op. cit.*, pp. 74-76.

În concluzie, la momentul în care încercăm să explicăm modul în care s-ar putea constitui şi stabili un consimţământ valabil în spatele tranzacţiilor realizate, trebuie să includem în algoritm reguli specifice şi nu generale, astfel încât să se poată realiza o ofertă veridică care, odată transmisă, va reda voinţa părţii faţă de care actul final va produce efecte. În cadrul teoriei reprezentării, odată încheiat contractul de către reprezentant, acesta va produce efecte faţă de partea – reprezentată fără a fi necesar ca aceasta să îşi fi exprimat consimţământul. S-au acordat doar câteva instrucţiuni algoritmului de către una dintre părţi[37]. Oferta şi acceptarea sunt schimbate între algoritm (ofertant) şi acceptant. În acest caz, intenţia de a contracta a algoritmului nu va putea fi explicată decât ca pe un posibil transfer de intenţie dinspre ofertant spre algoritm (transfer indirect).

A doua opinie, favorabilă teoriei contractuale, se foloseşte de mecanismul ofertă-acceptare pentru a explica problema consimţământului. Oferta este creată de partea implicată, care o va introduce în algoritm. Acesta va transmite oferta celuilalt posibil contractant realizând un transfer direct de voinţă de a contracta.

Odată îndeplinite aceste condiţii de formare ale contractului, fie pe cale de negociere, fie prin mecanismul ofertă-acceptare, inclusiv consimţământul părţilor, se poate vorbi despre un contract format în mod legal, obligatoriu pentru părţile sale.

Însumând cele anterior menţionate, observăm că nu este exclus ca, în anumite situaţii, algoritmul să poată fi perceput ca pe un reprezentat, iar programatorul, utilizatorul, fabricantul să fie consideraţi reprezentanţi ai acestuia. Cu toate acestea, la momentul în care se va alege teoria reprezentării drept teorie dominantă va trebui a fi avută în vedere reprezentarea legală. Bineînţeles că s-au formulat critici la adresa acestei opinii, respectiv, faptul că omul va putea deveni reprezentant, în vreme ce algoritmul nu va putea să primească o atare denominaţiune fără a avea personalitate juridică[38]. Astfel, de *lege ferenda*, s-ar impune o modificare a legii în sensul permiterii utilizării reprezentării drept instrument juridic capabil să explice rolul algoritmului în cadrul procesului de încheiere a contractului.

4. Moduri de căutare a secvenţelor de text în interiorul contractelor

În cele ce urmează vor fi prezentate variate modalităţi prin care algoritmul să fie utilizat în sfera contractuală fie pentru a ajuta părţile în crearea consimţământului, fie pentru a eficientiza procesul de încheiere a contractului sub aspectul variabilei temporale. Astfel, pentru a înţelege procesul prin care un algoritm poate găsi o secvenţă de caractere într-un text, trebuie mai întâi să înţelegem un proces mai simplu, prin care un algoritm poate să găsească un număr întreg în interiorul unui şir de numere întregi. Varianta cea mai simplă este de a

[37] *Ibidem.*

[38] V. Ooi, *Contracts formed by software: An approach from the law of mistake*, în *Centre for AI & Data Governance*, 2019, p. 9, [Online] la https://ink.library.smu.edu.sg/ caidg/3, accesat 11.10.2021.

parcurge şirul, element cu element şi de a ne opri odată ce numarul căutat este găsit. Cu toate acestea, timpul de căutare creşte în raport cu mărimea şirului de elemente. Spre exemplu, pentru a parcurge 10^9 elemente, adică un miliard de elemente ale şirului, un calculator modern are nevoie de 15 secunde. Pentru a parcurge 10^12 elemente, calculatorului îi trebuie 4 ore şi 10 minute, iar pentru a parcuge 10^18 elemente, calculatorul are nevoie de 475 de ani[39]. Acum să ne întrebăm câte caractere apar într-un contract. Este fiabil să folosim acest algoritm de căutare pentru a găsi o secvenţă de litere dintr-un contract în timp util?

În acest sens, a devenit utilizat algoritmul căutarii binare. Pentru a înţelege căutarea binară, pornim, de asemenea, de la un exemplu. Astfel, să presupunem că folosim şirul numerelor naturale cuprinse între 1 şi 1024. Numărul pe care îl căutam este 1024. Dacă trasăm mijlocul acestui şir, adică 512, ne punem întrebarea dacă numărul căutat este mai mare sau mai mic decât mijlocul. 1024 este mai mare decât 512, deci vom căuta doar în a doua jumătate a şirului iniţial. Următorul pas este acela de a găsi noul mijloc al şirului de numere aflate între 512 si 1024, adică 768. Repetăm pasul anterior şi observăm faptul că 1024 este mai mare decât 768, deci restrângem căutarea la a doua jumătate a şirului. Vom repeta aceşti paşi până când ajungem la numărul 1024. Astfel, până la pasul final, vor fi parcurşi doar 10 paşi, comparativ cu 1023 de paşi care ar fi fost parcurşi în cazul abordării primului algoritm[40].

În situaţia prezentată ne folosim de exemplul unui şir crescător de numere întregi. Cu toate acestea, pentru a putea funcţiona algoritmul căutării binare va fi necesar un şir de numere sau caractere ordonat. Astfel, în cazul unui contract, cum ar putea algoritmul să identifice prezenţa unor cuvinte cheie sau a unor secvenţe de text predefinite? Una dintre soluţiile acestei probleme este împărţirea contractului în unităţi mai mici. Presupunând că pornim de la un singur paragraf al contractului, acesta în interiorul algoritmului, poate fi sortat într-o ordine alfabetică, pentru a putea fi căutat cuvântul dorit în interiorul secvenţei de cuvinte. Această sortare se poate face în mai multe modalităţi. Cea mai uşoară rezolvare constă în compararea cuvintelor două câte două şi interschimbarea acestora în cazul în care nu se aflau deja în ordine alfabetică. Această metodă de sortare se realizează prin interclasare. Cu ajutorul acestei metode, putem ordona atât cuvinte, cât şi propoziţii, pentru a putea folosi ulterior algoritmul căutării binare.

[39] G.L. McDowell, *Cracking the Coding Interview 6th Edition,* Editura CareerCup, Palo Alto, 2019, pp. 38-39.

[40] *Idem,* p. 149.

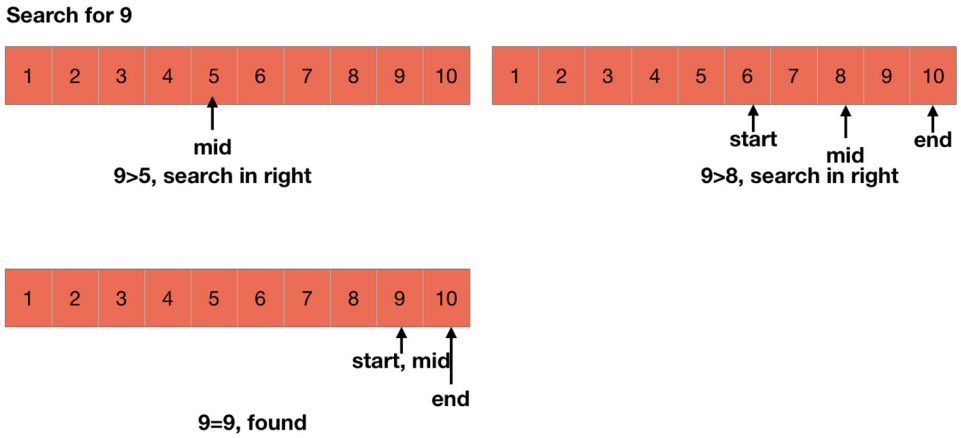

Fig. 1. Căutarea binară[41]

Un alt mod de utilizare a algoritmului în sfera contractuală se referă la recunoaşterea semnăturilor. Astfel, pentru a putea recunoaşte o semnătură, un algoritm trebuie ca, în prealabil, să primească drept date de intrare respectiva semnătură în format electronic, spre exemplu un fişier „.png" ce conţine un model al semnăturii. Astfel, printr-un algoritm de recunoaştere a imaginii, pot fi detectate toate semnăturile unui individ din interiorul unui contract.

Recunoaşterea unui obiect dintr-o fotografie sau dintr-o filmare se poate realiza cu niveluri mai mari sau mai mici de acurateţe, în funcţie de tipul de informaţie pe care algoritmul doreşte să îl extragă. Există două funcţii pe care recunoaşterea imaginilor le poate îndeplini, acestea fiind: clasificarea şi segmentarea.

Clasificarea se referă la identificarea unei „clase", adică a unei categorii în care poate fi încadrată o imagine. Fiecare imagine poate avea o singură clasă[42].

Segmentarea se referă la localizarea unui element dintr-o imagine în funcţie de pixelii identificaţi. Astfel, pentru unele cazuri, într-un algoritm de recunoaştere a imaginilor, se pune accent pe principiul segmentării. Unul dintre aceste cazuri este identificarea semnăturilor pe un contract, întrucât chiar şi o mică diferenţă faţă de original, ar putea semnala o semnătură falsă. Folosindu-se de nuanţa pixelilor din interiorul unei imagini, algoritmul poate localiza cu exactitate o semnătură pe pagina unui contract.

[41] [Online] la https://www.codesdope.com/course/algorithms-binary-search/, accesat 16.10.2021.

[42] V. Mititelu, *Recunoașterea imaginilor în baza indicilor de moment*, p. 3, [Online] la https://ibn.idsi.md/sites/default/files/imag_file/469-472_1.pdf, accesat 15.10.2021.

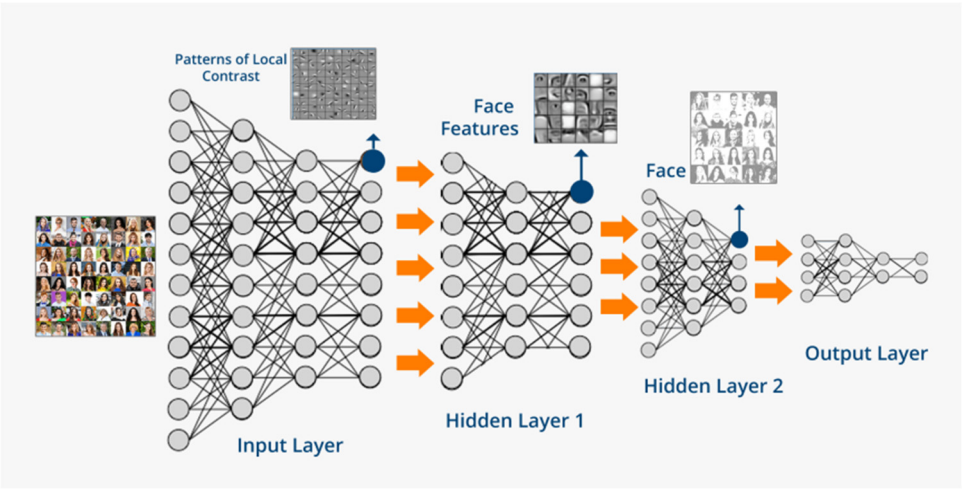

Fig. 2. Reţea neuronală[43]

Recunoaşterea imaginilor are la bază conceptul de *„Deep Learning”*, care se referă la un set de tehnici de învăţare automate. Acestea funcţionează cu ajutorul unor reţele neuronale artificiale. O reţea neuronală aritificială funcţionează similar cu creierul unui om. Aceasta este formată din mai multe straturi, complexitatea depinzând de tipul de informaţie pe care algoritmul trebuie sa o extragă. În esenţă, o reţea neuronală artificială este doar o funcţie matematică ce necesită date de intrare şi parametri pentru a putea oferi datele de ieşire. Datele de ieşire, în cazul nostru, constau atât în informaţii cu privire la validitatea semnăturilor unui individ din cadrul unui contract, cât şi în numărul de semnături ale respectivei persoane. Astfel, se poate observa cu uşurinţă dacă semnăturile sunt originale sau dacă toate clauzele contractului au fost semnate.

În practică, pentru a utiliza acest algoritm în identificarea semnăturilor unei persoane într-un contract, reţeaua neuronală artificială trebuie sa treacă printr-un proces de învăţare. Un set de imagini trebuie să fie colectate şi introduse ca date de intrare. Odată ce acest set de date a fost creat este esenţial ca, pentru fiecare imagine, programatorul să îi spună algoritmului dacă în ea se află sau nu obiectul căutat, împreună cu locaţia sa. După ce tot setul de date de intrare a trecut deja prin acest proces, urmează ca algoritmul să înceapă învăţarea. Reţeaua neuronală trebuie să înveţe un concept prin trecerea peste un număr mare de exemple.

Scopul final al acestui întreg proces este acela de a crea un algoritm care poate spune cu exactitate dacă semnătura unui individ din cadrul unui contract a fost falsificată sau este originală.

Utilitatea unui astfel de algoritm poate fi extinsă şi la aflarea numărului de semnături din cadrul unui contract, cu scopul de a trece peste citirea contractului

[43] [Online] la https://www.researchgate.net/figure/Structure-of-a-deep-neural-net-DNN-for-facial-recognition-6_fig2_325530258, accesat 16.10.2021.

mai eficient. Astfel, îmbinând algoritmul căutarii binare cu o reţea neuronală artificială care detectează prezenţa semnăturilor unui individ, se poate realiza citirea corectă a unui contract într-un timp foarte scurt.

Algoritmul va putea, de asemenea, să fie perceput drept fundament al contractelor inteligente. Acestea sunt programe pentru calculator, respectiv, protocoale de tranzacţie destinate să execute, să controleze sau să documenteze automat evenimentele şi acţiunile relevante din punct de vedere juridic în conformitate cu termenii unui contract sau ai unui acord. Obiectivele contractelor inteligente sunt reducerea nevoii de intermediari de încredere şi a costurilor de executare, precum şi reducerea oricăror altor costuri[44].

Din perspectiva programatorului, un astfel de contract va purta denumirea de „*smart contract*" dacă, odată ce a fost transferat în format electronic, acestuia i se poate aplica un algoritm care să eficientizeze procesul de încheiere a respectivului act. Spre exemplu, acesta poate parcurge în întregime şi identifica toate clauzele contractului într-o perioadă de timp semnificativ mai scurtă decât un om sau poate identifica tentativele de falsificare a semnăturilor cu o precizie mult mai mare decât un om.

Printre primele tehnologii care aplică un algoritm ce poate fi asemănat cu un algoritm dintr-un „*smart contract*" se află tonomatele de cafea. Algoritmul din spatele unui simplu tonomat de cafea este foarte uşor de implementat întrucât aparatul, în orice moment, se poate afla doar în una dintre cele patru situaţii:

1. Tonomatul are suficient credit introdus în el şi are suficientă cafea, ceea ce rezultă în dispensarea cafelei şi încheierea contractului.

2. Tonomatul are suficient credit introdus în el, dar nu are suficientă cafea, caz în care nu se poate încheia contractul dintre algoritm şi cumpărător.

3. Tonomatul nu are suficient credit introdus în el şi are suficientă cafea, moment în care algoritmul cere sa fie indroduşi mai mulţi bani.

4. Tonomatul nu are suficient credit indrodus în el şi nu are suficientă cafea, ceea ce duce din nou la imposibilitatea încheierii unui contract între algoritm şi om.

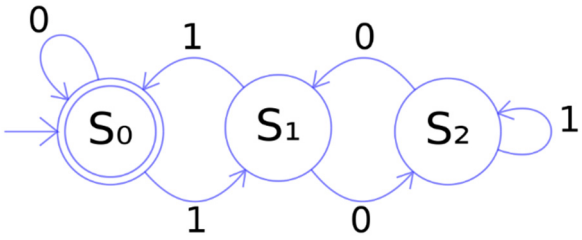

Fig. 3. *Finite state automata*[45]

[44] R. Herian, *Smart contracts: a remedial analysis,* în *Information & Communications Technology Law*, 2020, lucrare utilizată integral, [Online] la https://www.tandfonline.com/doi/abs/10.1080/13600834.2020.1807134, accesat 17.10.2021.

[45] [Online] la https://dndimitri.eu/2020/02/09/deterministic-finite-state-automota-for-regular-expres, accesat 16.10.2021.

Astfel, pe baza unui algoritm ce trece doar prin patru cazuri simple, se poate crea un contract între un om şi o maşinărie. Cu toate acestea, ce se întâmplă în cazul în care cineva a depus suficient credit în tonomat, dar nu mai există cafea pentru a fi dispensată? Algoritmul nu prevede o soluţie pentru un asemenea caz. Cu toate acestea, algoritmul care este folosit la un contract smart este cu mult mai avansat decât cel folosit la un simplu tonomat de cafea. Pentru a putea controla şi identifica toate posibilele situaţii care pot interveni în procesul de încheiere al unui contract, un algoritm ar produce un număr foarte mare de posibile scenarii care să aibă loc.

5. Concluzii

Având în vedere cele expuse putem conchide faptul că algoritmul poate avea statutul de participant în procesul de încheiere a contractului, dar răspunsul nu este unul absolut, ci nuanţat în funcţie de opţiunea părţilor. Acestea îl pot privi drept un reprezentant al voinţei lor şi care va crea o ofertă în raport cu termenii şi limitările generale impuse de subiectul reprezentat. O a doua soluţie pentru care pot opta părţile este aceea de a respecta cadrul legal şi de a folosi mecanismul ofertei-acceptării în vederea aducerii în prim-plan a consimţământului real al viitorilor contractanţi. Cu alte cuvinte, îmbinând regula de drept cu interesul părţii, se creează o soluţie care să explice, de fapt, ceea ce doresc părţile a realiza prin intermediul contractului.

Referinţe

Bob M.D., *Manual elementar de drept privat roman*, Editura Universul Juridic, Bucureşti, 2019

Chopra S., White L.F., *Artificial Agents and the Contracting Problem: A Solution Via an Agency Analysis*, în *University of Illinois Journal of Law Technology & Policy*, 2010

Gaius, *Instituţiunile*, trad. Aurel N. Popescu, Editura Academiei Republicii Socialiste România, Bucureşti, 1982

Gellers J.C., *Rights for Robots. Artificial Intelligence, Animal and Environmental Law*, Editura Routledge, New York, 2021

Herian R., *Smart contracts: a remedial analysis*, în *Information & Communications Technology Law*, 2020, https://doi.org/10.1080/13600834.2020.1807134

Hogg M., *Promises and Contract Law. Comparative Perspectives*, Editura Cambridge University Press, The Edinburgh Building, Cambridge, 2011

McDowell G.L., *Cracking the Coding Interview 6th Edition*, Editura CareerCup, Palo Alto, 2019

Oliver M., *Contracting by artificial intelligence: open offers, unilateral mistakes, and why algorithms are not agents*, în *ANU Journal of Law and Technology*, Vol. 2, 2021

Ooi V., *Contracts formed by software: An approach from the law of mistake*, în *Centre for AI & Data Governance*, 2019, http://dx.doi.org/10.2139/ssrn.3322308

Pagallo U., *The Laws of Robots: Crimes, Contracts, Torts*, Editura Springer Science+Business Media Dordrecht, Dordrecht Heidelberg New York London, 2013

Pop L., Popa I.F., Vidu S.I., *Curs de drept civil. Obligaţiile*, Editura Universul Juridic, Bucureşti, 2015

Quinot G., *Offer, Acceptance, and the Moment of Contract Formation*, *in loc. cit.*, Hector MacQueen, Reinhard Zimmermann, *European Contract Law. Scots and South African Perspectives*, Editura Edinburgh University Press, Edinburgh, 2006

Reier Forradellas R.F., *Digital Transformation and Artificial Intelligence Applied to Business: Legal Regulations, Economic Impact and Perspective*, în *Laws*, 2021, https://doi.org/10.3390/laws10030070

Scholz L.H., *Algorithmic Contracts*, în *Stan. Tech. L. Rev.*, nr. 128, Stanford, California, 2017

Supiot A., *Homo juridicus: eseu despre funcţia antropologică a dreptului*, Editura Rosetti Educational, Bucureşti, 2011

Ungureanu C.T., *Drept civil. Partea generală. Persoanele*, Editura Hamangiu, Bucureşti, 2013

Van Beers B., *The Changing Nature of Law's Natural Person: The Impact of Emerging Technologies on the Legal Concept of the Person*, German Law Journal, Vol. 18, No. 03, https://doi.org/10.1017/S2071832200022069

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-14

Perspective curente de semnare a contractelor online în dreptul comparat

Current Perspectives for Online Contracts Signing in the Comparative Law

Andreea-Luminiţa Buţureanu-Cărpuşor[1]

Rezumat: Posibilitatea semnării contractelor în variantă electronică este o practică răspândită cu mult înainte de începutul pandemiei COVID-19 la nivel global şi continuă să faciliteze relaţiile dintre părţi, prestarea de servicii şi obţinerea de profituri. În ciuda posibilităţii de semnare frauduloasă a contractelor, încheierea online aduce beneficii importante în reducerea birocraţiei şi pentru relaţiile comerciale internaţionale. Lucrarea de faţă îşi propune să delimiteze specificul semnării contractelor online în România şi Marea Britanie. Scopul acestui demers comparativ este atât de a evidenţia oportunităţile oferite de legislaţia actuală, cât şi de a identifica potenţiale îmbunătăţiri legislative locale prin raportare la legislaţia britanică. În prima parte, discutăm despre legislaţia ţării noastre şi tipurile de contracte care se pretează semnării online. În partea a doua, problematizăm semnarea contractelor online în Marea Britanie.

Cuvinte-cheie: contractele online în România; contractele online în Marea Britanie; practica judiciară a contractelor online

Abstract: The possibility of signing contracts electronically is a widespread practice long before the onset of the global COVID-19 pandemic and continues to facilitate relations between the parties, the provision of services and the making of profits. Despite the possibility of fraudulent signing of contracts, online conclusion brings important benefits in reducing bureaucracy and for international trade relations. This paper aims to delimit the specifics of signing online contracts in Romania and the United Kingdom. The purpose of this comparative approach is both to highlight the opportunities offered by current legislation and to identify potential local legislative improvements in relation to British legislation. In the first part, we discuss the legislation of our country and the types of contracts that are suitable for signing online. In the second part, we question the signing of online contracts in the UK.

Keywords: online contracts in Romania; online contracts in the UK; judicial practice of online contracts

[1] Doctorand, Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iaşi, e-mail: bnpcarpusor2021@gmail.com.

1. Contractele online în România

Contractul reprezintă înţelegerea formală şi scrisă dintre două părţi care are rolul de a consfinţi între acestea realitatea instituirii unor drepturi şi/sau obligaţii între acestea. Dintr-o perspectivă mai nuanţată, putem spune faptul că fiecare contract are rolul de a fi un reper în timp şi o piedică împotriva uitării drepturilor şi/sau responsabilităţilor care decurg din acesta - *„verba volant, scripta manent"*.

Utilizarea semnăturii electronice şi a contractelor online este susţinută de statul român prin următoarele reglementări: art. 1245 din Codul civil, art. 267 şi 268, alineatul 2) din Codul de procedură civilă din România, Legea nr. 455/2001 privind semnătura electronică, normele tehnice şi metodologice de aplicarea Legii nr. 455/2001 privind semnătura electronică, Legea nr. 451/2004 privind marca temporală, Ordinul MCSI nr. 492/2009 privind normele tehnice şi metodologice pentru aplicarea Legii nr. 451/2004 privind marca temporală, Legea nr. 135/2007 privind arhivarea documentelor în formă electronică, Ordinul MCSI nr. 493/2009 privind normele tehnice şi metodologice pentru aplicarea Legii nr. 135/2007 privind arhivarea documentelor în formă electronică, Ordonanţa de urgenţă a Guvernului nr. 34/2014 privind drepturile consumatorilor în ceea ce priveşte contractele la distanţă, Legea nr. 365/2002 privind contractele încheiate prin mijloace electronice şi Ordonanţa de Urgenţă nr. 36 din 5 mai 2021.

În prezent, următoarele tipuri de contracte deja fac obiectul semnării online, cu sau fără semnătură electronică calificată în practica românească: contractul de muncă (începând din anul 2018), de vânzare-cumpărare, contractul de credit, de antrepriză, de arendare, contractul de joc şi pariu. Pe baza semnăturii electronice simple sau calificate (de tip *DocuSign* sau *certSIGN*), şi contractele de locaţiune, de comodat şi de arendare pot fi semnate online, cu condiţia depunerii unei copii a contractului la primăria din raza locuinţei şi a bunurilor arendate. În egală măsură, opinăm că, dacă vânzarea şi prestarea de servicii pot face obiectul unor contracte semnate electronic, şi contractele de întreţinere, respectiv donaţie, se pot bucura de acelaşi regim.

În ciuda popularităţii sporite a semnăturii electronice calificate, Regulamentul UE *eIDAS* subliniază, printre altele, un aspect important, anume că un document electronic nu poate fi refuzat ca probă pe motiv că nu este semnat electronic calificat[2].

Fiind un regulament al UE, *eIDAS* este obligatoriu şi se aplică direct în sistemul juridic naţional. *eIDAS* are prioritate faţă de Legea nr. 455/2001, şi oferă posibilităţi mai extinse faţă de aceasta. În orice caz, *eIDAS* se bazează pe principiul conform căruia efectul juridic al semnăturilor electronice este definit de legislaţia naţională, cu excepţia cerinţei conform căreia o semnătură electronică calificată ar trebui să aibă efectul juridic echivalent al unei semnături scrise de mână[3].

[2] Paragraful 63 din Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE.

[3] Paragraful 49 din preambulul eIDAS.

În mod fundamental, semnătura electronică este definită ca un cumul de date în formă electronică care sunt ataşate sau asociate logic cu alte date în formă electronică şi care sunt utilizate de semnatar pentru a semna[4]. Sunt reglementate trei tipuri de semnături electronice:

▪Semnătura electronică simplă - constă în date în formă electronică care sunt ataşate sau asociate logic cu alte date în formă electronică şi care sunt utilizate de semnatar pentru a semna. De pildă, semnătura utilizată într-un e-mail sau semnătura dată pe anumite tampoane digitale pentru semnături[5].

▪Semnătura electronică extinsă, denumită semnătură electronică avansată („AES") în eIDAS - este semnătura electronică care: este legată în mod unic de semnatar, permite identificarea semnatarului, este creată folosind date de creare a semnăturii electronice pe care semnatarul le poate utiliza, cu un nivel ridicat de încredere, sub controlul său exclusiv; şi este legată de datele semnate cu acesta, astfel încât orice modificare ulterioară a datelor să fie detectabilă[6].

Semnătura electronică extinsă bazată pe un certificat calificat, denumită semnătură electronică calificată (QES), este o semnătură electronică avansată creată de un dispozitiv de creare a semnăturii electronice calificate şi care se bazează pe un certificat calificat pentru semnături electronice.

Distincţia semnificativă dintre AES şi QES constă în faptul că aceasta din urmă este generată de un dispozitiv calificat de creare a semnăturilor electronice. Acest element suplimentar ale QES are rolul de a întări identitatea semnatarului, motivul pentru care QES este considerat cel mai sigur tip de semnătură electronică, cu o valoare legală superioară. Totuşi, aşa cum am precizat, lipsa unei semnături electronice calificate nu atrage după sine nulitatea unui contract online[7]. Este important de precizat că în ţara noastră contractele semnate online fac obiectul legislaţiei doar din perspectiva formării lor.

În practică, însă, contractului încheiat la distanţă nu îi sunt recunoscute pe deplin efectele. În ciuda faptului că un contract poate fi încheiat prin telefon sau pe internet, fără cerinţa unei semnături olografe sau electronice, în cazul unui litigiu, un contract astfel încheiat este privit ca unul deficitar. Recunoaşterea deplină a efectelor şi punerea în executare silită par uneori privilegii rezervate doar clasicelor contracte redate prin înscrisuri sub semnătura privată sau chiar autentice, singura concesie fiind cea în favoarea contractelor semnate prin semnătura electronică extinsă. Un exemplu elocvent în acest sens îl constituie practica neunitară a

[4] C. Constantinescu, *Semnătura electronică – relații (comerciale) la distanță*, Juridice.ro, 2020, [Online] la https://www.juridice.ro/680846/semnatura-electronica-relatii-comerciale-la-distanta.html, accesat 02.11.2021.

[5] Ș. Grigorescu, *The electronic signature: long-distance (commercial) relationships*, 2020, Bpv-grigorescu.com, [Online] la https://www.bpv-grigorescu.com/news/the-electronic-signature-long-distance-commercial-relationships/, accesat 04.11.2021.

[6] *Ibidem.*

[7] CertSIGN, *Semnătura electronică şi contractul la distanţă, în justiţie. Valide sau nu?*, CertSIGN.ro, 2020, [Online] la https://www.certsign.ro/ro/semnatura-electronica-si-contractul-la-distanta-in-justitie/, accesat 05.11.2021.

instanţelor de judecată în ceea ce priveşte caracterul de titlu executoriu al contractelor de servicii financiare încheiate la distanţă. Pe de o parte, au fost instanţe de judecată care au apreciat că un contract de credit încheiat cu respectarea prevederilor O.G. nr. 85/2004 privind protecţia consumatorilor la încheierea şi executarea contractelor la distanţă privind serviciile financiare poate constitui titlu executoriu chiar dacă el nu cuprinde semnătura olografă sau, după caz, semnătura electronică extinsă a debitorului. Pe de altă, au existat instanţe care au considerat că acele contracte de furnizare de servicii de credit încheiate la distanţă care nu conţin semnătura olografă sau, după caz, semnătura electronică extinsă a debitorului nu constituie titluri executorii[8].

O recentă decizie a Înaltei Curţi de Casaţie şi Justiţie pronunţată într-un recurs în interesul legii (Decizia nr. 23/2019) tranşează această problemă aducând o schimbare clară de optică. Astfel, instanţa supremă a decis în favoarea recunoaşterii caracterului de titlu executoriu cu privire la contractele de servicii financiare încheiate la distanţă cu respectarea strictă a dispoziţiilor legale speciale, chiar în lipsa semnăturii olografe sau a semnăturii electronice extinse, cu excepţia situaţiei în care părţile impun semnătura drept condiţie de validitate a contractului[9].

În susţinerea deciziei sale, Î.C.C.J. subliniază că, de vreme ce norma specială care reglementează încheierea contractelor la distanţă, respectiv O.G. nr. 85/2004, nu prevede nicio obligaţie în sarcina părţilor contractante de a semna convenţia încheiată, această condiţionare nu poate fi impusă suplimentar pentru a recunoaşte acestor contracte caracterul de titlu executoriu consacrat pentru contractele de credit prin art. 52 alin. (1) din Legea nr. 93/2009 şi art. 120 din O.U.G. nr. 99/2006[10].

Mai mult, Î.C.C.J. atrage atenţia că o astfel de condiţionare „ar fi chiar în contradicţie cu mecanismul încheierii contractelor la distanţă, *inter absentes*, precum şi cu specificul contractelor referitoare la servicii financiare, la comerţul electronic, bazat pe celeritate şi pe lipsa formalismului, contractele de acest gen ţinând de activitatea comercială şi fiind funciarmente contracte care se încheie *solo consensu*”[11].

Prin aceeaşi decizie, instanţa supremă a statuat şi că un contract încheiat la distanţă, cu respectarea regulilor incidente, reprezintă un înscris pe suport informatic, mijloc de probă distinct şi se bucură de prezumţia de validitate a înscrierii şi de putere doveditoare în condiţiile Codului de procedură civilă[12].

[8] A. Jivan, *Contractul la un click distanță*, Economica.net, 2013, [Online] la https://www.economica.net/contractul-la-un-click-distan-a-avoca-ii-explica-ce-riscuri-aduc-contractele-electronice-foarte-utilizate-in-contextul-pandemiei-de-coronavirus_183864.html, accesat 07.11.2021.

[9] *Ibidem.*

[10] *Ibidem.*

[11] Înalta Curte de Casație și Justiție, Decizia nr. 23 din 14 octombrie 2019, publicată în Monitorul Oficial nr. 142 din 21 februarie 2020.

[12] *Ibidem.*

Putem concluzia că, deşi Decizia nr. 23/2019 reprezintă fără îndoială un pas înainte în sprijinul consolidării eficacităţii contractelor încheiate la distanţă, rămân, în continuare, de actualitate problemele legate de proba contractului încheiat la distanţă. Astfel, conform art. 282-283 din Codul de procedură civilă, un act juridic ale cărui date există iniţial doar pe suport informatic poate fi probat printr-un document care reproduce respectivele date doar dacă acel document este inteligibil şi prezintă garanţii suficient de serioase pentru a face deplină credinţă în privinţa conţinutului acestuia şi a identităţii persoanei de la care acesta emană. În ce constau acele garanţii, dacă sunt ele suficient de serioase – sunt aspecte ce rămân la aprecierea instanţei de judecată care va decide de la caz la caz, ţinând cont de circumstanţele în care datele au fost înscrise şi de documentul care le-a reprodus.

De asemenea, prezumţia de valabilitate a înscrierii menţionată în Decizia nr. 23/2019 este şi ea condiţionată de cerinţa ca înscrierea să fie făcută în mod sistematic şi fără lacune, iar datele înscrise să fie protejate contra alterărilor şi contrafacerilor astfel încât integritatea documentului să fie deplin asigurată[13].

Prin urmare, în cadrul legal actual, jurisprudenţa are un rol esenţial în asigurarea eficacităţii contractelor încheiate la distanţă, instanţele fiind chemate să asigure un just echilibru între protecţia reală a intereselor părţilor, a consumatorilor în primul rând şi nevoia acceptării şi utilizării pe scară largă a contractelor încheiate în mediul virtual.

Până la consolidarea unei jurisprudenţa unitare care să ofere criterii clare, însă, în ciuda atitudinii încurajatoare a instanţei supreme, participanţii la comerţul online, şi în special profesioniştii, trebuie să fie conştienţi de riscurile pe care le implică încheierea contractelor la distanţă şi să ia masurile necesare pentru diminuarea acestora. Astfel, este de dorit ca profesioniştii să structureze cu atenţie procedurile de vânzare on-line, să aleagă cu grijă sistemele informatice pe care le folosesc şi să respecte întocmai normele legale speciale aplicabile în funcţie de tipul de produse sau servicii pe care le oferă[14].

2. Contractele online în Regatul Unit al Marii Britanii şi Irlandei de Nord

În spaţiul britanic, cu excepţia contractelor care oferă posibilitatea transferului de drepturi privind proprietăţile imobiliare, toate categoriile de contracte pot face obiectul semnării online[15], iar următoarele prevederi reglementează acest aspect:

[13] *Ibidem.*

[14] *Ibidem.*

[15] A. Ruwanthika, *Protecting consumer rights in electronic contracts: a lesson from the European Union and the United Kingdom*, 11th International Research Conference, General Sir John Kothalawala Defence University, September 13th -14th 2018, Conference Proceedings, 2018. [Online] la https://www.researchgate.net/publication/349552079_PROTECTING_CONSUMER_RIGHTS_IN_ELECTRONIC_CONTRACTS_A_LESSONS_FROM_EUROPEAN_UNION_AND_UNITED_KINGDOM, accesat 02.11.2021.

▪Regulamentul privind comerţul electronic din 2002 (Regulamentul privind comerţul electronic) impune operatorilor de site-uri comerciale o serie de obligaţii, în special obligaţii de a furniza utilizatorilor anumite informaţii despre operator şi serviciile acestuia.

▪Consumer Rights Act 2015 (CRA) a consolidat o serie de legislaţii anterioare din Marea Britanie privind drepturile consumatorilor şi a actualizat anumite domenii, inclusiv condiţiile legale implicite din contractele consumatorilor şi remediile pentru încălcări disponibile consumatorului.

▪Regulamentul privind contractele de consum (informaţii, anulare şi taxe suplimentare) din 2013 (Regulamentul privind contractele de consum) impune obligaţii suplimentare operatorilor de site-uri web care se ocupă de consumatori, precum şi introducerea drepturilor de anulare pentru consumatori.

▪Reglementările din 2008 privind protecţia consumatorilor împotriva tranzacţiilor neloiale (CPR) interzic diverse practici neloiale ale comercianţilor, precum acţiuni sau omisiuni înşelătoare şi includ o „listă neagră" de practici comerciale interzise.

▪Regulamentul privind furnizarea de servicii din 2009 (regulamentele POS) prevede că, în furnizarea de servicii, comercianţii nu trebuie să facă discriminări între rezidenţii SEE pe motive de naţionalitate sau locul de reşedinţă, cu excepţia cazului în care este justificat de criterii obiective (de exemplu, furnizarea de servicii transfrontaliere implică anumite costuri adiţionale).

▪GDPR şi Legea privind protecţia datelor 2018 (DPA) conţin prevederi referitoare la utilizarea datelor cu caracter personal, inclusiv cu privire la utilizatorii site-ului web.

▪Regulamentele din 2003 privind confidenţialitatea şi comunicaţiile electronice (Directiva CE) din 2003 (Regulamentele PEC) reglementează marketingul direct (atât solicitat, cât şi nesolicitat) prin intermediul comunicării electronice.

Se poate observa faptul că, dincolo de formarea contractului, legislaţia britanică are în vedere mai multe aspecte privind contractele online, precum informarea şi protecţia consumatorilor, împreună cu practicile neloiale care pot apărea şi sunt desemnate o serie de instituţii pentru protecţia părţilor în cazul încălcării prevederilor care ţin de buna executare a contractelor.

Totodată, în spaţiul anglo-saxon, contractul de arendare face obiectul semnării online în mod explicit şi se specifică faptul că dacă arendatorul semnează contractul de arendare şi îl expediază arendaşului spre a fi semnat, se poate presupune că arendaşul are la dispoziţie mai mult timp pentru a studia condiţiile contractuale, însă, în acelaşi timp, în această perioadă arendaşul poate abandona semnarea contractului. Această situaţie ar prejudicia interesul arendatorului deoarece perioada de timp în care terenul său nu este fructificat se reflectă în

pierderi de ordin financiar. Se impune, astfel, ca primul semnatar al contractului de arendare să fie arendaşul[16].

Pentru ca un contract online să aibă efecte, trebuie să existe o ofertă, acceptare, intenţia de a crea relaţii juridice şi certitudinea termenilor. Oferta, acceptarea şi încorporarea termenilor sunt de o importanţă deosebită atunci când se realizează contracte online.

Pentru a oferi comerciantului control asupra termenilor contractului, termenii şi condiţiile unui site web adesea afirmă că, prin trimiterea unei comenzi, clientul face o ofertă, şi descrie termenii în care se consideră că comerciantul a acceptat oferta respectivă, de exemplu, numai după ce a trimis clientului un e-mail de confirmare a comenzii.

Termenii contractului trebuie aduşi suficient la cunoştinţa clientului înainte de finalizarea contractului. Instanţele engleze nu au oferit îndrumări definitive cu privire la modul în care trebuie încorporaţi termenii şi condiţiile online, dar au evidenţiat faptul că cel mai eficient mod de a proiecta site-ul web este astfel încât clientul să nu poată finaliza comanda până când nu a derulat termenii şi condiţiile complete de pe ecran şi a făcut click pe un buton de „Accept" (sau similar). Acest lucru este cunoscut sub numele de contract *click-wrap*. În contextul acordurilor de licenţă software (cunoscute sub numele de acorduri de licenţă pentru utilizatorul final) există alte două forme comune de contract:

- Contracte *browse-wrap*, în care un utilizator este pur şi simplu notificat că, continuând să utilizeze software-ul, acesta va fi obligat de anumiţi termeni şi condiţii, dar fără ca acesta să fie nevoit să ia o acţiune pozitivă pentru a-i accepta.

- Contracte de reducere, în cazul în care un utilizator achiziţionează un produs software fizic şi termenii sunt fie incluşi în ambalaj, fie într-un fişier care trebuie să fie deschis în timpul instalării[17].

Concluzii

Posibilităţile de semnare online a contractelor din România sunt, în prezent, mult mai variate decât se cunoaşte şi se anunţă a fi o practică mult mai răspândită în lumina regulamentului eIDAS. Reţinem faptul că, în ciuda popularităţii sporite a semnăturii electronice calificate, un aspect important este că un document electronic nu poate fi refuzat ca probă pe motiv că nu este semnat electronic calificat. Totodată, dacă legislaţia românească tinde să accentueze aspectele legate de formarea contractului în formă electronică, cea britanică detaliază atât tipurile de contracte online posibile, cât şi informarea şi protecţia consumatorilor, împreună cu practicile neloiale care pot apărea şi sunt desemnate o serie de instituţii pentru protecţia părţilor în cazul încălcării prevederilor care ţin de buna

[16] A.H. Adenuga, C. Jack, R. McCarry, *The Case for Long-Term Land Leasing: A Review of the Empirical Literature*, Land, Nr.10/ 2021, 238, [Online] la https://doi.org/10.3390/land10030238, accesat 29.10.2021.

[17] E. McKendrick, L. Qiao, *Contract Law*, Ediția a 13-a, MacMillan Law, 2019, p. 82, Kindle edition.

executare a contractelor. În viitorul apropiat, ar fi importantă reglementarea tuturor aspectelor legate de contractele online şi în legislaţia românească, în virtutea realităţilor pandemice.

Referinţe

Adenuga A.H., Jack C., McCarry R., *The Case for Long-Term Land Leasing: A Review of the Empirical Literature*, Land, Nr.10/ 2021, 238, https://doi.org/ 10.3390/land10030238

Constantinescu C., *Semnătura electronică – relaţii (comerciale) la distanţă*, Juridice.ro, 2020, [Online]

CertSIGN, *Semnătura electronică şi contractul la distanţă, în justiţie. Valide sau nu?*, CertSIGN.ro, 2020, [Online]

Grigorescu Ş., *The electronic signature: long-distance (commercial) relationships*, 2020, Bpv-grigorescu.com, [Online]

Înalta Curte de Casaţie şi Justiţie, Decizia nr. 23 din 14 octombrie 2019, publicată în Monitorul Oficial nr. 142 din 21 februarie 2020

Jivan A., *Contractul la un click distanţă*, Economica.net, 2013, [Online]

McKendrick E., Qiao L., *Contract Law*, Ediţia a 13-a, MacMillan Law, 2019, Kindle edition

Puie O., *Tratat de contracte civile potrivit Codului civil, Codului de procedură civilă, Codului fiscal, Codului de procedură fiscală, Codului penal şi Codului de procedură penală*, Volumul I, Editura Universul Juridic, Bucureşti, 2018

Romoşan I.D., *Obligaţii*, Editura Universul Juridic, Bucureşti, 2018

Ruwanthika A., *Protecting consumer rights in electronic contracts: a lesson from the European Union and the United Kingdom*, 11th International Research Conference Proceedings, General Sir John Kothalawala Defence University, September 13th -14th 2018

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-15

Uberizarea dreptului – pericol sau oportunitate pentru profesiile juridice liberale?

Uberization of Law – Danger or Opportunity for the Liberal Legal Professions?

Cătălin Boacnă[1]

Rezumat: Termenul de „*uberizare*” a devenit prezent în limbajul uzual al ultimilor ani, odată cu extinderea celebrei firme americane de *ride-sharing*. Principiul de bază este acela că o aplicaţie informatică instalată pe telefonul mobil poate crea legătura dintre un conducător auto independent şi un client care evită serviciile de taximetrie. Criza sanitară provocată de coronavirus a accentuat *uberizarea* unor domenii precum piaţa muncii, medicină, IT etc. În acest context, apreciez că termenul poate fi folosit în mod adecvat şi în ceea ce priveşte dreptul. Există deja platforme care oferă servicii juridice online sau intermediază legătura dintre client şi avocat. De asemenea, unele softuri legislative pot înlocui sfaturile juridice ale unui avocat sau pot prevedea rezultatul unui proces prin folosirea unor algoritmi. În acest context, *uberizarea* dreptului reprezintă un pericol sau o oportunitate pentru contractul de asistenţă juridică definit de Legea nr. 51/1995 privind organizarea şi exercitarea profesiei de avocat?

Cuvinte-cheie: uberizarea dreptului; contractul de asistenţă juridică; digitalizare; platforme juridice

Abstract: The term uberization has become present in the usual language of recent years, with the expansion of the famous american ride-sharing company. The basic principle is that an application installed on the mobile phone can create the connection between an independent driver and a customer who avoids taxi services. The health crisis caused by coronavirus has accentuated the uberization of areas such as the labor market, medicine, IT etc. In this context, I belive that the term can also be used appropriately in terms of law. There are already platforms that offer legal services online or mediate the connection between the client and the lawyer. Also, some legislative software can replace the legal advice of a lawyer or can predict the outcome of a lawsuit by using algorithms. In this context, does the uberisation of law represent a danger or an opportunity for the legal aid contract defined by Law no. 51/1995 on the organization and exercise of the lawyer profession?

Keywords: uberization of law; legal aid contract; digitization; legal platforms

[1] Doctorand, Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iaşi, e-mail: catalin_boacna@yahoo.com.

1. Introducere

Modul de funcţionare a platformei americane de *ride-sharing*[2] Uber a dat naştere unor controverse intense încă din momentul lansării[3], atât din punct de vedere al modelului de afacere, cât şi din punct de vedere juridic. Criticii companiei susţin că în jurul acestei platforme a fost construită o adevărată „cultură a ilegalităţii"[4], modelul de afaceri bazându-se pe încălcarea legii la nivel global, nu doar în SUA. Pe de altă parte, admiratorii susţin, printre altele, că a revitalizat economia[5] sau că a adus inovaţii tehnologice, care au schimbat soarta serviciilor tradiţionale, nu doar cele din domeniul taximetriei[6]. În acest context, a apărut termenul „*uberizare*", un neologism care descrie „actul sau procesul de schimbare a pieţei pentru un serviciu prin introducerea unui mod diferit de cumpărare sau utilizare a acestuia, în special folosind tehnologia mobilă"[7] sau, mai clar, se referă la „oferirea de servicii directe prin intermediul unei aplicaţii mobile"[8]. Practic, astăzi, în vorbirea uzuală, termenul „*uberizare*" nu se mai referă doar la conduita unui utilizator al aplicaţiei „Uber" de a căuta o maşină disponibilă care să-l ducă din punctul A în punctul B, ci se referă la un fenomen social care a cuprins toate domeniile esenţiale, de la economie până la medicină, muzică, turism, piaţa muncii, educaţie, sau chiar domeniul juridic. *Uberizarea* reprezintă un adevărat fenomen social, iar dreptul este obligat să aibă o reacţie. Cea mai clară reacţie a fost aceea că legislaţiile naţionale şi-au schimbat treptat perspectiva şi au introdus în cotidian inovaţiile tehnologice bazate pe modelul platformei americane de *ride-sharing*.

2. Uberizarea dreptului

„*Uberizarea* dreptului" este o sintagmă pe care încă nu am regăsit-o în limba română, deşi este deja prezentă, de exemplu, în limbajul juridic din Franţa[9]. Din punctul meu de vedere, termenul de *uberizare*, folosit pentru a descrie tehnologizarea domeniului juridic trebuie analizat în strânsă legătură cu noţiunea

[2] [Online] la https://en.wikipedia.org/wiki/Uber, accesat 10.12.2021.

[3] [Online] la https://www.forbes.com/sites/ellenhuet/2014/12/11/ubers-global-expansion/?sh=8d52806550a7, accesat 10.12.2021.

[4] [Online] la https://hbr.org/2017/06/uber-cant-be-fixed-its-time-for-regulators-to-shut-it-down, accesat 10.12.2021.

[5] [Online] la https://www.theatlantic.com/technology/archive/2019/03/what-happened-uber-x-companies/584236/, accesat 10.12.2021.

[6] [Online] la https://digital.hbs.edu/platform-digit/submission/uber-vs-taxi/, accesat 10.12.2021.

[7] [Online] la https://dictionary.cambridge.org/dictionary/english/uberization, accesat 10.12.2021.

[8] [Online] la https://www.cyberdefinitions.com/definitions/UBERIZATION.html, accesat 10.12.2021.

[9] [Online] la https://www.lemonde.fr/idees/article/2015/06/19/vers-une-uberisation-du-droit_4658065_3232.html, accesat 10.12.2021.

de dematerializare a dreptului[10] sau dematerializarea procesului judiciar[11]. Definirea *dematerializării* este mai poetică în dicţionarul explicativ al limbii franceze[12] decât cea din limba română, însă esenţa este aceeaşi: „dematerializarea" se defineşte ca fiind acţiunea de a elimina ceea ce este material pentru a rămâne doar partea imaterială[13]. Evoluţia tehnologică, dar mai ales modalitatea în care algoritmii vor controla procesul judiciar şi vor elimina partea materială, pare a fi o prioritate atât pentru politica globală a Uniunii Europene[14] cât şi pentru legislaţia naţională a statelor europene[15]. Astfel, *uberizarea* dreptului nu va reprezenta doar un mecanism de utilizare a unei aplicaţii informatice pentru a găsi un avocat potrivit pentru un anumit domeniu, pentru a căuta legi, contracte, sau pentru a depune o acţiune la instanţa de judecată, ci va putea reprezenta un mijloc prin care un justiţiabil poate afla verdictul potenţial al unui anumit dosar. Practic, algoritmii vor putea previziona hotărârea judecătorului, iar părţile litigiului respectiv îşi vor putea face aşteptări realiste de la actul de justiţie. *Uberizarea* dreptului se va realiza în mod treptat, chiar şi forţat[16], cu opoziţie din partea profesioniştilor, în toate sistemele juridice ale ţărilor dezvoltate şi va schimba radical procesul judiciar tradiţional[17], având în vedere tocmai experienţa trăită în ceea ce priveşte intrarea pe piaţa mondială a companiei Uber. Deşi în realitate compania oferă servicii specifice taximetriei[18], iar şoferii independenţi care folosesc aplicaţia sunt în

[10] M. Dochy, *La dématérialisation des actes du procès civil*, Volumul 202, pg. 3, Editura Dalloz, Paris, 2021.

[11] Această noțiune apare Opinia Nr.(2011)14 a CCJE – „Justiţia şi Tehnologiile Informatice (IT)", Adoptată de CCJE în cadrul celei de a 12-a sesiuni plenare, Strasbourg, 7-9 Noiembrie 2011.

[12] "*réduire en esprit*" - É. Littré, Dictionnaire de la langue française - vb *Dématérialiser* **vs** DEX - *Dematerializa* dematerializez, vb. I. Tranz. și refl. A face să piardă sau a pierde caracteristicile materiei sau chiar materia. [Pr.: -ri-a-] – Din fr. *dématérialiser*.

[13] C. Rocayaura, *Réflexions sur la dématérialisation de la procédure pénale*, thèse, Montpellier 1, 2013, no 3.

[14] *Carte albă privind inteligența artificială - O abordare europeană axată pe excelență și încredere*, Bruxelles, 19.2.2020. Este vorba de un proiect de regulament prezentat la data de 21 aprilie 2021 de Comisia Europeneană, fiind considerat ca fiind prima propunere din lume pentru un cadru legal în ceea ce privește Inteligența Artificială (IA).

[15] Cu ocazia Summit-ului, despre inteligență artificială, martie 2018, Paris, președintele Franței a anunțat strategia națională de cercetare în inteligență artificială, fiind anunțate inclusiv schimbări legislative în acest sens.

[16] N. Fricero, *Demande en justice et nouvelles technologies : aspects* procéduraux, în *Les avocats dans le monde numérique : qu'en est- il aujourd'hui ?*, *Procédures*, nr 10, 2014, dosar 47.

[17] C. Chainais, F. Ferrand, L. Mayer, S. Guinchard, *Procédure civile : droit interne européen du procès civil*, Editura Dalloz, colecția Précis Dalloz, ediția 34, Paris, 2018, pg. 947: "La dématérialisation des procédures entraîne un bouleversement de nos habitudes et envahit peu à peu toute la vie judiciaire".

[18] Analiza modului în care funcționează compania Uber a fost realizată de către Curtea de Justiție a Uniunii Europene în Cauza C-434/15 Asociación Profesional Elite Taxi împotriva Uber Systems Spain SL, pronunțată la data de 20 decembrie 2017.

realitate angajaţii Uber[19], politica de expansiune a fost aceea că oferă servicii specifice domeniului IT punând la dispoziţia utilizatorilor o simplă aplicaţie prin care clienţii îşi pot găsi o maşină, iar conducătorii auto îşi pot găsi clienţi. Pe acelaşi raţionament, în viitorul apropiat, aplicaţiile informatice nu vor oferi doar o intermediere între profesioniştii dreptului şi clienţi, ci vor putea oferi chiar răspunsul la problemele juridice pe care le are clientul respectiv. În ultimii ani există destul de multe exemple concrete prin care statele europene au încercat să digitalizeze inclusiv rolul concret al judecătorului, exemplul cel mai notoriu fiind cel al Estoniei – un program informatic ce judecă litigiile civile cu valoarea de până în 6400 Euro[20].

După cum am arătat, criza sanitară provocată de coronavirus a accentuat *uberizarea* unei game largi de domenii. Aş da ca exemplu piaţa muncii, acolo unde ştim cu toţii că există anumite reguli foarte stricte în ceea ce priveşte programul de lucru, forma contractului de muncă (care trebuie înregistrată la Inspectoratul Teritorial de Muncă), durata contractului, sarcinile de serviciu, fişa postului etc. Odată cu dezvoltarea aplicaţiilor informatice, ajungem în situaţia în care o platformă online poate genera nu doar oferte de muncă şi cereri din partea celor care caută, ci poate reprezenta activitatea în sine[21]. *Uberizarea* muncii a început cel mai clar în domeniul IT, unde există platforme prin intermediul cărora se pun la dispoziţia utilizatorilor oferte de lucru sau utilizatorii pun la dispoziţia angajatului produsul muncii lor. În domeniul turismului, lucrurile sunt şi mai clare pentru că acolo există platforme de tipul booking.com (companie înfiinţată în anul 1996 în Olanda), care pun la dispoziţia turiştilor locuri de cazare, iar unităţile de cazare îşi găsesc clienţii. Acelaşi principiu îl regăsim şi în domeniul artistic sau muzical. Nu mai suntem nevoiţi să cumpărăm un disc de vinil pentru a asculta o melodie veche, ci o găsim pe diferite platforme. Filmele nu mai rulează doar în cinema sau la TV, ci avem la dispoziţie platforme de *streaming* care facilitează activităţile noastre recreative. De asemenea, putem găsi şi medici pe internet, care mai nou oferă consultaţii medicale de la distanţă. În acelaşi timp, au apărut inclusiv aplicaţii informatice care pot da, cu precizie maximă, diagnostice medicale.

3. Uberizarea în raport cu profesiile liberale – avocatura

Firmele de taxi sunt în pericol din cauza Uber, sistemul bancar este ameninţat de dezvoltarea criptomonedelor, retailerii au probleme serioase din cauza

[19] Intervenţia instanţelor de judecată din majoritatea statelor Europene au cosiderat că şoferii care folosesc aplicaţia sunt, în concret, angajaţii Uber, cu toate drepturile şi obligaţiile care decurg din acest statut.

De exemplu, [Online] la https://www.lepoint.fr/justice/le-lien-entre-uber-et-un-chauffeur-requalifie-en-contrat-de-travail-21-05-2021-2427556_2386.php, accesat 10.12.2021.

[20] [Online] la https://www.lefigaro.fr/secteur/high-tech/en-estonie-une-intelligence-artificielle-va-rendre-des-decisions-de-justice-20190401, accesat 10.12.2021.

[21] [Online] la https://republica.ro/uberizarea-muncii-de-ce-munca-ar-ramane-ca-acum-100-de-ani-8-ore-pe-zi-5-zile-pe-saptamana, accesat 10.12.2021.

platformelor online de vânzări de tipul Amazon sau Emag, agenţiile de turism sunt ameninţate de platformele de tip booking.com sau Airbnb.com, iar televiziunea clasică are o problemă serioasă cu audienţa din cauza dezvoltării platformelor de tipul Tiktok, Netflix sau Youtube. Bineînţeles, exemplele pot continua. În acest context, ar fi cu totul nefiresc ca dreptul să nu intre sub umbrela fenomenului descris mai sus. În mod particular, contractul de asistenţă juridică încheiat între un avocat şi un client poate suferi modificări esenţiale. Din acest punct de vedere, Legea nr. 51/1995 privind organizarea şi exercitarea profesiei de avocat deţine unele reglementări care par în afara *uberizării* actuale. Există deja platforme care oferă servicii juridice[22] online sau care intermediază legătura dintre client şi avocat[23], iar unele soft-uri pot înlocui sfaturile unui avocat prin folosirea de algoritmi bazaţi pe experienţe anterioare[24]. Christiane Féral-Schuhl[25], fost preşedinte al Consiliului Naţional al Barourilor din Franţa, avocat în dreptul noilor tehnologii, susţine în volumul „Cyberdroit" că dezvoltarea platformelor online este un ajutor real pentru profesie: „avocatul, la fel ca un medic, este singurul autorizat să depună un diagnostic legal. Cu toate acestea, trebuie să folosească aceste noi instrumente pentru a răspunde mai bine nevoilor justiţiabililor şi pentru a se adapta la noile lor constrângeri în societatea digitală. La fel ca medicul, aceste instrumente îi vor permite să-şi gestioneze altfel profesia, dar subliniind valoarea adăugată care este de neînlocuit: diagnosticul. Unii văd aceste schimbări ca pe o ameninţare pentru avocat. De altfel, dacă expresia *uberizare* este recentă, procesul a început imediat ce a apărut internetul. Secretarii caselor de avocatură au fost primele victime, unele dintre sarcinile lor fiind „absorbite" treptat de avocaţi. Prin urmare, implementarea serviciilor juridice online este o extensie a unui proces de lungă durată"[26].

Astăzi, raportat la toate cele menţionate mai sus, poate fi de neînţeles prevederea regăsită în conţinutul art. 245 din Statutul profesiei de avocat cu privire la faptul că firma unui cabinet de avocatură trebuie să aibă dimensiunile maxime de 40 X 60 cm, să aibă o amplasare strictă sau că trebuie să cuprindă anumite menţiuni gravate în mod obligatoriu pe un suport metalic[27]. Această prevedere are

[22] [Online] la https://www.acjsfb.ro/2021/02/16/parteneriatul-dintre-inteligenta-artificiala-si-profesiile-juridice-un-salt-urias-pentru-omenire/, accesat 10.12.2021.

[23] [Online] la https://www.zf.ro/business-hi-tech/platforma-avocatura-com-95-dintre-clienti-prefera-consultanta-video-18925207, accesat 10.12.2021.

[24] [Online] la https://www.wolterskluwer.com/ro-ro/expert-insights/ai-sau-nu-ai-in-avocatura, accesat 10.12.2021.

[25] [Online] la https://www.cnb.avocat.fr/fr/christiane-feral-schuhl-presidente-du-cnb, accesat 10.12.2021.

[26] C. Féral-Schuhl, *Cyberdroit 2020/2021 - 8e* ed.: *Le droit à l'épreuve de l'internet*, Editura Praxis Dalloz, Paris, 2020.

[27] Articolul 245 din Statul profesiei de avocat Statutul profesiei de avocat din 3 decembrie 2011 (actualizat).

„(1) Firma trebuie să aibă dimensiunile maxime de 40 x 60 cm şi va fi amplasată la intrarea imobilului şi/sau a spaţiului ocupat în care forma de exercitare a profesiei îşi are sediul profesional principal sau secundar ori biroul de lucru.

legătură cu publicitatea în cadrul profesiei de avocat. Prin hotărârea nr. 195/11.09.2021 pentru modificarea şi completarea Statutului profesiei de avocat, adoptat prin Hotărârea Consiliului Uniunii Naţionale a Barourilor din România (UNBR) nr. 64/2011[28], publicată în Monitorul Oficial nr. 1055 din 4 noiembrie 2021, Uniunea Naţională a Barourilor din România a înţeles că acest tip de exprimare nu trebuie să-şi mai găsească locul în Statutul profesiei şi astfel, art. 245, menţionat anterior, a fost abrogat. În schimb, conţinutul art. 245 se regăseşte la punctul 6 din *Ghidul de bune practici privind publicitatea avocatului şi a formelor de exercitare a profesiei*, îmbrăcând forma unei recomandări. În concret, acest *Ghid* preia aproape integral tot ceea ce se regăsea la secţiunea privind publicitatea din statutul profesiei de avocat. Articolele 244-250 care privesc modul în care avocatul poate să-şi facă publicitate, dar mai ales interdicţiile cu privire la acest aspect, au fost abrogate cu totul odată cu intrarea în vigoare a Hotărârii nr. 195/11.09.2021. Deşi majoritatea restricţiilor privind publicitatea avocatului au fost mutate din statut în *Ghidul* elaborat de UNBR, interdicţia care se regăsea în conţinutul art. 244, alin. (2), lit. b[29] nu a mai fost preluată în Ghidul de bune practici. Norma menţionată interzicea în mod expres acordarea de consultaţii juridice pe orice suport material sau prin orice mijloc de comunicare în masă, cu excepţia rubricilor juridice din diverse publicaţii.

În mod evident, o platformă informatică la care are acces un număr nelimitat de utilizatori este un mijloc de comunicare în masă şi astfel, se poate înţelege cu uşurinţă că practica avocaţilor care ofereau consultanţă juridică pe *Tik-tok* sau prin postări de tip *live* pe reţelele de socializare era interzisă. Această interdicţie a fost radiată pur şi simplu din statut şi nepreluată în Ghidul menţionat mai sus. În acest context, intervine o întrebare firească: în acest moment, poate avocatul să acorde consultanţă juridică pe reţelele de socializare ca şi cum s-ar afla pe o scenă de spectacol, iar utilizatorii ar dori răspunsuri la problemele lor juridice? Acest tip de retorică va naşte cu siguranţă polemici şi tensiuni în interiorul profesiei. Articolul care interzicea în mod expres acest fapt a fost abrogat, fapt care oferă un răspuns pozitiv la întrebarea anterioară. În schimb, rămâne în discuţie contractul de asistenţă juridică, forma în care trebuie încheiat, limitele de acţiune şi conţinutul acestuia. Articolul 108[30] din Statutul profesiei, regăsit la secţiunea privind relaţia

(2) Firma cuprinde menţiunile prevăzute în anexa nr. XXII, gravate pe suport metalic".

[28] [Online] la http://legislatie.just.ro/Public/DetaliiDocument/247907, accesat 10.12.2021.

[29] *„(2) Nu este permisă utilizarea următoarelor forme de publicitate:*

b) acordarea de consultații și/sau redactarea de acte juridice, realizate pe orice suport material, precum și prin orice alt mijloc de comunicare în masă, inclusiv prin emisiuni radiofonice sau televizate, cu excepția publicațiilor care conțin o rubrică de consultanță juridică;".

[30] Articolul 108

„(1) Dreptul avocatului de a asista, a reprezenta ori a exercita orice alte activități specifice profesiei se naște din contractul de asistență juridică, încheiat în formă scrisă între avocat și client ori mandatarul acestuia.

(2) Forma, conținutul și efectele contractului de asistență juridică sunt stabilite prin prezentul statut.

dintre avocat şi client, arată destul de clar că avocatul nu poate acorda asistenţă juridică fără existenţa unui contract de asistenţă juridică încheiat în formă scrisă. Art. 121 alin. 5 din Statutul profesiei permite încheierea contractului de asistenţă juridică în formă verbală, doar sub rezerva redactării contractului în forma scrisă în cel mai scurt timp. În acelaşi timp, potrivit art. 121 alin. (1), contractul de asistenţă juridică dobândeşte dată certă la momentul în care este înregistrat în registrul de evidenţă a contractelor, contractul fiind unicul mijloc de probă al raporturilor dintre client şi avocat (art. 122, alin. 7).

Protecţia oferită de contractul de asistenţă juridică trebuie să fie reciprocă ambelor părţi semnatare în sensul că, de exemplu, avocatul trebuie să-şi definească limitele mandatului şi să-şi monetizeze prestaţia, iar clientul trebuie să aibă un mijloc de protecţie împotriva unor eventuale sfaturi greşite din partea avocatului, nefiind valabilă asigurarea profesională în contextul unor consultaţii juridice pe internet, în public, fără existenţa unui contract. Practic, condiţia încheierii unui contract de asistenţă juridică îl împiedică pe avocat să poată acorda asistenţă juridică prin intermediul reţelelor de socializare sau a aplicaţiilor informatice care permit accesul unui număr nelimitat de utilizatori. În schimb, acordarea unor sfaturi juridice generale, nepersonalizate, poate reprezenta o formă de atragere a unor eventuali clienţi. Aparent este un tip de publicitate permisă de Statutul profesiei, deşi ar putea exista interpretări privind interzicerea acesteia dacă este asimilată unor forme de publicitate mascată[31].

Lipsa de armonie între reglementările specifice profesiei de avocat şi evoluţia platformelor informatice de tipul Uber a fost oarecum corectată prin Hotărârea nr. 195/11.09.2021 a UNBR în sensul că a fost elaborat pe lângă *Ghidul de bune practici* şi *Ghidul privind utilizarea platformelor online de către avocaţi*. Acest ghid acoperă o necesitate a pieţei juridice, platformele online de intermediere a serviciilor avocaţilor existau, dar nu erau reglementate. În România, acest ghid a apărut pe fondul crizei sanitare generate de Covid-19, dar şi ca urmare a Ghidului privind utilizarea platformelor online[32], elaborat de către Consiliul Barourilor Europene în iunie 2018. Permisiunea de a acorda consultanţă juridică prin intermediul platformelor online trebuie asimilată în mod obligatoriu cu posibilitatea mai facilă de a contracta, de a încheia un contract de asistenţă juridică cu fiecare client în parte, iar nu cu posibilitatea avocatului de a acorda consultanţă juridică oricărui

(3) Avocatul nu poate acționa decât în limitele contractului încheiat cu clientul său, cu excepția cazurilor prevăzute de lege".

[31] Art. 2.6 din *Ghidul privind utilizarea platformelor online de către avocați*: Publicitatea mascată constă în reprezentarea prin cuvinte sau imagini a serviciilor, numelui, mărcii ori activităților avocatului sau formelor de exercitare a profesiei, în cazul în care o astfel de reprezentare este destinată unor scopuri publicitare nedeclarate și poate induce în eroare publicul cu privire la natura sa. Astfel de reprezentări sunt considerate intenționate mai ales atunci când se fac în schimbul unei plăți sau al unei contraprestații.

[32] [Online] la https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Guides_recommendations/EN_DEON_20180629_CCBE-Guide-on-lawyers-use-of-online-legal-platforms.pdf, accesat 10.12.2021.

utilizator de internet, oricum, în orice condiţii. În plus, art. 120 alin. (1) din Statutul profesiei interzice acordarea de consultanţă juridică fără ca anterior avocatul să verifice identitatea exactă a clientului său ori a persoanei care contractează în numele acestuia. Este imposibil de realizat acest lucru în momentul în care un avocat acordă asistenţă juridică simultan unui număr mare de abonaţi ai unei reţele de socializare. Prin intermediul unei platforme juridice este de asemenea o misiune dificilă. De exemplu, partea adversă într-un litigiu îşi face un cont fals şi cere consultanţă juridică avocatului. Poate comunicarea pe internet să ofere o astfel de protecţie şi să asigure independenţa avocatului? Răspunsul este discutabil, însă, fiecare platformă are specificul ei, modalităţi diferite de interacţiune între client şi avocat.

4. Tipuri de platforme informatice specifice avocaturii

Ghidul CCBE privind utilizarea platformelor online de către avocaţi publicat în iunie 2018[33] şi introdus ca anexă la Statutul profesiei de avocat din România în noiembrie 2021 arată că există diferenţe destul de mari între platformele informatice destinate avocaturii.

a. Platforme care conţin registre cu avocaţi

Acest tip de site-uri oferă un registru destul de amplu cu avocaţii care se înscriu sau care sunt înscrişi pe platformă, de cele mai multe ori contra unei sume de bani. Platformele create de organele de conducere ale profesiei din ţările Europene sunt gratuite. Este vorba de site-uri de tipul www.find-a-lawer.com. Sunt inserate datele de identificare ale avocaţilor, cu specializarea fiecăruia, iar clienţii pot găsi avocatul potrivit în funcţie de anumite filtre prestabilite. De obicei, pe acest tip de site nu există interacţiune între avocat şi client, acesta din urmă având posibilitatea să îl contacteze în mod direct, nemijlocit. În dreptul european, aceste platforme sunt denumite „anuare", iar în dreptul anglo-saxon sunt descrise sub termenul „directoare". Aceste registre sunt gratuite pentru avocaţi. De cele mai multe ori, aceştia sunt înscrişi acolo fără să-şi dorească în mod expres asta.

b. Platformele de recomandare ale avocaţilor

Acest tip de site asigură o conexiune cu dublu sens între avocaţi şi clienţi. Dacă în primul caz clienţii căutau avocatul potrivit prin inserarea unor filtre stabilite în funcţie de specializare, experienţă şi localizare, platformele de recomandare oferă şi posibilitatea avocaţilor de a găsi clienţi noi. De obicei, aceste platforme conţin mai multe informaţii despre avocaţii înscrişi, dar şi modalităţi tehnice prin care profesionistul să răspundă, să interacţioneze într-un timp foarte scurt cu utilizatorul care are nevoie de servicii juridice. Aceste site-uri reprezintă de multe ori un atac direct la etica şi deontologia profesională pentru că oferă clasamente şi comparaţii între avocaţi, fiind lipsite de transparenţă în ceea ce priveşte ordinea în care sunt selectaţi avocaţii care apar pe prima pagina. Există şi

[33] [Online] la https://www.unbr.ro/ghidul-ccbe-privind-utilizarea-platformelor-online-de-catre-avocati/, accesat 10.12.2021.

un risc real în ceea ce priveşte manipularea opiniei publice având în vedere că sunt finanţate atât de reclamele generate de numărul cât mai mare de utilizatori, cât şi de abonamentul pe care îl plătesc avocaţii înscrişi.

c. Platforme de întrebări şi răspunsuri în domeniul juridic

Aceste site-uri sunt foarte populare în rândul utilizatorilor care vor să afle cât mai rapid opinia unui profesionist. Obiectivul acestor platforme nu este acela de a pune în legătură avocaţii cu clienţii pentru încheierea unor contracte de asistenţă juridică, ci doar pentru a-şi putea creşte traficul de internet şi, implicit, pentru a obţine mai mulţi bani din reclame. În acelaşi timp, pentru avocaţi pot reprezenta un punct de pornire într-o eventuală relaţie de colaborare cu un client. Practic, avocatul oferă clientului un răspuns incomplet la o anumită întrebare, iar pentru o consultanţă elaborată, clientul va trebui să semneze contractul. În cazul altor site-uri de acest tip, clienţii sunt cei care trebuie să achite un abonament lunar pentru a avea acces la comunitatea juridică şi a putea pune întrebări.

d. Platformele de tip „robotlawyers"

Aceste platforme informatice oferă răspunsuri prestabilite la întrebări juridice uzuale. Pun la dispoziţia utilizatorilor un serviciu bazat pe inteligenţa artificială care poate să iniţieze şi să întreţină o scurtă conversaţie juridică. Pentru că aceşti „roboţi de conversaţie" nu pot funcţiona ca un avocat adevărat, pot direcţiona utilizatorul către un avocat specializat în domeniul solicitat. Aceste platforme pot reprezenta o oportunitate pentru avocaţi având în vedere că pot înlocui personal uman care răspunde la întrebări uzuale şi nu necesită cunoştinţe de IT foarte solide.

e. Platforme care oferă şabloane şi automatizări de documente

Reprezintă un instrument modern de eficientizare a activităţii unui cabinet de avocatură. Acest tip de platformă este destinat în principal cabinetelor sau societăţilor de avocatură pentru a uşura activitatea internă. Pare mai degrabă un produs dezvoltat exclusiv de profesionişti în informatică decât de jurişti. Programul este capabil să construiască modele de contracte, sau să creeze documentaţii necesare funcţionării unei societăţi. În acelaşi timp, poate crea modele de formulare destinate unei activităţi curente: înregistrarea unor firme, redactarea statutului unei asociaţii, plângeri sau cereri către instanţele de judecată etc.

5. Uberizarea avocaturii în context european

În România, fenomenul *uberizării* avocaturii s-a produs destul de târziu faţă de alte ţări europene, fapt recunoscut inclusiv de organele de conducere ale profesiei[34]. După cum am explicat anterior, există încă destul de multe inconsecvenţe în legislaţia specifică avocaturii, care pot conduce la concluzii de tipul: „cererile online se depun la camera 4 de la etajul 2". Această concluzie este întărită

[34] [Online] la https://www.bursa.ro/dike-supliment-dedicat-activitatii-de-drept-avocatura-se-38171uberizeaza38187-la-fel-ca-restul-serviciilor-69849448, accesat 10.12.2021.

inclusiv de faptul că acel *Ghid de bune practici* anexat *Statutului* oferă dreptul Consiliului Baroului să verifice conţinutul unui site deţinut de un avocat şi să elimine menţiunile care încalcă principiile esenţiale ale profesiei. Până la data publicării Hotărârii nr. 195/2021 în Monitorul Oficial şi simpla creare a unui site de prezentare a avocatului trebuia aprobată de Consiliul Baroului[35].

Prima ţară din Uniunea Europeană care a deschis calea acestei *uberizări* a profesiei a fost Franţa. Consiliul Naţional al Barourilor a pus la dispoziţia utilizatorilor două platforme de tipul celor descrise mai sus (un registru cu avocaţi[36] şi un site de recomandare[37]). Cele două platforme care pot fi accesate încă din anul 2016 sunt administrate în mod direct de către Consiliu. Platforma de recomandare a avocaţilor are filtre multiple prin care se asigură un contact cât mai rapid cu avocatul. Clientul poate iniţia un apel telefonic direct din aplicaţie, poate stabili o întâlnire la birou, o întâlnire video sau poate doar să adreseze o întrebare.

Decizia de a liberaliza în această manieră piaţa avocaturii vine în contextul tehnologizării agresive, dar şi în contextul Hotărârii Curţii de Justiţie a Uniunii Europene (CJUE) din data de 15 ianuarie 2015[38], prin care s-a stabilit că avocatul nu este doar un jurist veritabil, ci este un furnizor de servicii, iar clientul este un consumator. Această hotărâre a Curţii de Justiţie a produs un adevărat seism în domeniul juridic având în vedere că în interpretarea Directivei 93/13/CEE a Consiliului din 5 aprilie 1993 privind clauzele abuzive în contractele încheiate cu consumatorii[39], contractul de asistenţă juridică încheiat între un avocat şi un client este considerat a fi încheiat între un „furnizor" şi „un consumator". Practic, Curtea a oficializat caracterul pur comercial al contractului de asistenţă juridică prin faptul că este standardizat, conţinând clauze deja prestabilite de avocat sau de Statutul profesiei. După această decizie, fenomenul *uberizării* avocaturii a devenit tot mai intens.

În Italia, restricţiile privind publicitatea avocatului, prevăzute de Legea nr. 247 din 31.12.2012, publicată în Monitorul Oficial nr. 15 din 18 ianuarie 2013, sunt oarecum similare cu cele din România. Pe site-ul Consiliului Naţional al Barourilor din Italia este publicat un anuar/registru privind avocaţii, însă nu are alte filtre de căutare decât cele standard: nume, oraş şi specializare. Autorităţile din Italia nu au creat o platformă de tipul celei de recomandare, prin care clientul să poată interacţiona instant cu avocatul, uneori chiar prin sistem video. În schimb, există un număr foarte mare de astfel de platforme private, care oferă inclusiv clasamente

[35] *„(2) Conținutul și modul de prezentare a adresei de internet se avizează, în prealabil, de consiliul baroului și trebuie să respecte demnitatea și onoarea profesiei, precum și secretul profesional".*

[36] [Online] la https://www.cnb.avocat.fr/fr/annuaire-des-avocats-de-france, accesat 10.12.2021.

[37] [Online] la https://consultation.avocat.fr/, accesat 10.12.2021.

[38] [Online] la https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A62013CJ0537, accesat 10.12.2021.

[39] [Online] la https://eur-lex.europa.eu/legal-content/RO/LSU/?uri=celex:31993L0013, accesat 10.12.2021.

între avocaţi, *ranking*-uri, recomandări de la foşti clienţi, fenomenul luând amploare începând cu anul 2017[40]. Latura pur comercială a avocaturii în Italia pare a fi foarte dezvoltată având în vedere concurenţa mare din interiorul profesiei. Media este de 4,5 avocaţi la mia de locuitori ai Italiei[41] (în zone precum Calabria, chiar 7 la mie), o cifră mult mai mare decât în alte ţări europene. Pentru comparaţie, în România, media calculată la numărul avocaţilor care profesează şi sunt înregistraţi de UBNR[42] este de 1,15 avocaţi la mia de locuitori. O precizare importantă este aceea că în Italia există deja, începând cu anul 2018[43], mai multe platforme online care pun avocaţii în legătură între ei, nu doar cu clienţii. Mai exact, există platforme care intermediază legătura între avocaţi pentru găsirea rapidă a unor colaboratori, pentru substituirea în dosare sau pentru redactarea unor documente juridice.

În Germania, Legea Federală a Avocaţilor[44] permite utilizarea platformelor pentru interacţiunea dintre avocat şi client. Există inclusiv un Registru Naţional Oficial al Avocaţilor în care sunt trecute toate datele de contact ale avocaţilor, inclusiv filtre suplimentare legate de specializare sau titluri academice. În acelaşi timp, platformele private de tipul celor care recomandă avocaţi sunt foarte bine promovate în spaţiul virtual.

Referinţe

Dochy M., *La dématérialisation des actes du procès civil*, Volumul 202, pg. 3, Editura Dalloz, Paris, 2021

Féral-Schuhl C., *Cyberdroit 2020/2021 - 8e* ed.: *Le droit à l'épreuve de l'internet*, Editura Praxis Dalloz, Paris, 2020

Ferrand F., Mayer L., Guinchard S., Chainais C., *Procédure civile : droit interne européen du procès civil*, Editura Dalloz, colecţia Précis Dalloz, ediţia 34, Paris, 2018

Fricero N., *Demande en justice et nouvelles technologies: aspects* procéduraux, în *Les avocats dans le monde numérique : qu'en est- il aujourd'hui ?*, *Procédures*, nr. 10, 2014, dosar 47

Rocayaura C., *Réflexions sur la dématérialisation de la procédure pénale*, thèse, Montpellier 1, 2013, no 3

[40] [Online] la https://www.altalex.com/documents/news/2017/07/24/servizi-legali-il-fenomeno-dei-marketplace-digitali, accesat 10.12.2021.

[41] [Online] la https://nuvola.corriere.it/2019/12/24/quale-futuro-per-gli-avvocati/, accesat 10.12.2021.

[42] [Online] la https://www.ifep.ro/Justice/Lawyers/LawyersPanel.aspx, accesat 10.12.2021.

[43] [Online] la https://www.laleggepertutti.it/236186_lawe-la-prima-piattaforma-online-per-avvocati, accesat 10.12.2021.

[44] [Online] la https://www.brak.de/fuer-verbraucher/anwaltssuche/, accesat 10.12.2021.

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-16

Riscurile psihosociale întâlnite de salariaţi în economia digitală. Dreptul la deconectare

The Psychosocial Risks Encountered by Employees in the Digital Economy. The Right to Disconnect

Alexandra-Georgiana Vâlcelaru[1]

Rezumat: Deşi poate fi considerată drept răspunsul la multe dintre problemele cu care se confruntă părţile unui raport de muncă, munca digitală, indiferent de forma în care este prestată, expune lucrătorii la o serie de riscuri psihosociale, de natură a vătăma sănătatea fizică şi psihică, dar şi bunăstarea acestora. Cel mai concludent exemplu este oferit de pandemia de Sars-CoV-2, care a redefinit raporturile de muncă, dar a adus în prim-plan şi problema burnoutului cu care se confruntă lucrătorii digitali. În acest context, la nivel internaţional atât statele, prin intermediul modificărilor legislative, cât şi angajatorii, prin politicile interne încearcă să diminueze acest fenomen, una dintre cele mai importante măsuri adoptate fiind reglementarea dreptului la deconectare al lucrătorilor digitali.

Cuvinte-cheie: economia digitală; telemunca; munca pe platforme; dreptul la deconectare; burnout

Abstract: Although it can be considered as an answer to many of the problems faced by the parties of an employment relationship, digital work, regardless of the form in which it is performed, exposes workers to a number of psychosocial risks, such as harm to their physical and mental health, but also to their well-being. The most conclusive example is the one provided by the Sars-CoV-2 pandemic, which redefined employment relations, but also brought to the attention the problem of the burnout syndrome faced by the digital workers. In this context, internationally, both states, through ammendments of the legislation, and employees, through internal policies try to reduce the burnout phenomenon, one of the most important measures being the regulation of the digital workers right to disconnect.

Keywords: digital economy; telework; platform work; right to disconnect; burnout

1. Introducere

Potrivit OECD[2], *„economia digitală încorporează toată activitatea economică bazată pe sau îmbunătăţită semnificativ prin utilizarea intrărilor digitale, inclusiv*

[1] Doctorand, Facultatea de Drept, Universitatea din Bucureşti, e-mail: alexandra-georgiana.valcelaru@drept.unibuc.ro

[2] Organisation for Economic Co-operation and Development, *A roadmap toward a common framework for measuring the Digital Economy,* [Online] la https://www.oecd.org/

tehnologii digitale, infrastructură digitală, servicii digitale şi date. Se referă la toţi producătorii şi consumatorii, inclusiv guvernul, care utilizează aceste intrări digitale în activităţile lor economice".

În ceea ce priveşte digitalizarea, acesta reprezintă procesul de *„a transforma semnalele analogice în semnale digitale*"[3] sau, altfel spus, reprezintă *„utilizarea tehnologiilor digitale pentru a schimba un model de afaceri şi a oferi noi venituri şi oportunităţi de producere a valorii; este procesul de trecere la o afacere digitală"*[4].

Dat fiind că economia implică un ansamblu de activităţi umane desfăşurate în sfera producţiei, distribuţiei şi consumului bunurilor materiale şi serviciilor, o economie caracterizată de digitalizare implică nu doar trecerea la o afacere digitală, dar şi trecerea la o piaţă a muncii digitalizată.

Astfel, în prezent piaţa muncii este o reflexie a evoluţiei economiei, care se adaptează noilor cerinţe impuse de aceasta din urmă. Aşa cum concluzionează Eurofound[5], la acest moment există nouă tipuri generale de noi forme de ocupare a forţei de muncă, dintre care două considerăm că sunt caracteristice economiei digitale, respectiv munca mobilă bazată pe tehnologia informaţiei si comunicării[6] şi munca pe platformă[7], pe care le vom denumi generic în cele ce urmează *„munca digitală"*[8].

---

digital/ieconomy/roadmap-toward-a-common-framework-for-measuring-the-digital-economy.pdf, accesat 12.10.2021, pag 34, Arabia Saudită, 2020.

[3] Dicționarul Explicativ al Limbii Române, [Online] la https://dexonline.ro/definitie/digitaliza, accesat 12.10.2021.

[4] Gartner Glossary, [Online] la https://www.gartner.com/en/information-technology/glossary/digitalization, accesat 12.10.2021.

[5] I. Mandl, M. Curtarelli, S. Riso, O. Vargas, E. Gerogiannis, *New forms of employment*, European Foundation for the Improvement of Living and Working Conditions, Luxemburg, 2015: munca ocazională, *job-sharing, employee-sharing*, munca de portofoliu, managementul interimar, munca pe bază de vouchere, munca mobilă bazată pe tehnologia informației si comunicării, munca colaborativă și munca pe platformă.

[6] I. Mandl, M. Curtarelli, S. Riso, O. Vargas, E. Gerogiannis, *op. cit.*, pp. 118-123. Munca mobilă bazată pe tehnologia informației si comunicării se referă la munca prestată cel puțin parțial, dar în mod regulat, în afara *„biroului principal"*, fie că este sediul angajatorului sau un birou personalizat la domiciliu, folosind tehnologia informației si comunicării pentru conectarea online la sistemele informatice ale organizației. La nivel intern, acest tip de muncă este reprezentat de telemuncă, definită prin Legea nr. 81/2018 ca fiind *„forma de organizare a muncii prin care salariatul, în mod regulat şi voluntar, îşi îndeplineşte atribuţiile specifice funcţiei, ocupaţiei sau meseriei pe care o deţine în alt loc decât locul de muncă organizat de angajator, folosind tehnologia informaţiei şi comunicaţiilor".*

[7] I. Mandl, M. Curtarelli, S. Riso, O. Vargas, E. Gerogiannis, *op. cit.*, p. 107: *„este o formă de muncă în care se utilizează o platformă online pentru a permite organizațiilor sau indivizilor să acceseze un grup nedefinit și necunoscut de alte organizații sau alți indivizi pentru a rezolva probleme specifice sau pentru a furniza servicii sau produse specifice în schimbul unei remunerații".* Cele mai reprezentative forme de muncă în economia de tip *gig* sunt munca virtuală (așa-numitul „crowdworking") și munca colaborativă (cunoscută și ca munca la cerere prin aplicații).

[8] G. Ilie, A-M. Vlăsceanu, *Poate legislația muncii să țină pasul cu noua realitate economică?*, [Online] la https://www.hotnews.ro/stiri-specialisti_deloitte-23037203-poate-

Munca digitală a fost definită la rândul său, în literatura de specialitate ca fiind *„organizarea experienţei umane cu ajutorul creierului uman, a mediilor digitale şi a comunicaţiilor în aşa fel încât să fie create produse noi”*[9].

Având în vedere specificul său, respectiv utilizarea instrumentelor digitale ca principal mijloc de realizare a atribuţiilor, munca digitală reprezintă un avantaj important atât pentru angajatori, cât şi pentru lucrători în actualul context economic, dar şi în actualul context sanitar. Cu toate acestea, munca digitală implică o serie de riscuri psihosociale pentru lucrători.

2. Beneficiile muncii digitale

În ceea ce îi priveşte pe lucrători, un prim avantaj al muncii digitale îl reprezintă creşterea productivităţii lor, ca urmare a lipsei întreruperilor inerente muncii prestate la birou. De asemenea, aceştia se bucură de un echilibru mai bun între viaţa profesională şi viaţa personală, de reducerea stresului asociat navetei, de posibilitatea de a realiza economii ca urmare a reducerii costurilor legate de cheltuielile generate de nevoia unui vehicul, parcare sau transport public, îmbrăcăminte pentru lucru, alimente şi asigurări, dar şi de creşterea gradului de autonomie şi de flexibilitate.

Pe de altă parte, în ceea ce priveşte beneficiile aduse angajatorilor, printre acestea se numără: extinderea posibilităţii de a identifica salariaţi calificaţi, reducerea răspândirii bolilor şi posibilitatea lucrătorilor bolnavi de a-şi continua munca în afara locului lor obişnuit de muncă, reducerea costurilor, a consumului de energie şi a amprentei de carbon, posibilitatea de desfăşurare a activităţii pe mai multe fusuri orare şi creşterea adaptabilităţii culturale, reducerea fluctuaţiei personalului şi a absenteismului, acoperirea locurilor de muncă în caz de evenimente meteorologice extreme, când lucrătorii nu ar putea ajunge la locul de

legislatia-muncii-tina-pasul-noua-realitate-economica.htm, accesat 11.10.2021: *„munca virtuală implică folosirea unei platforme informatice pentru a identifica persoane care utilizează Internetul (i.e. crowdsourcing) și care sunt dispuse să presteze în spațiul virtual (i.e. crowdwork) o activitate retribuită ce constă în realizarea unor sarcini rezultate din divizarea unei activități mai complexe în părți componente ce se pot realiza succesiv și foarte rapid (e.g. codificare, procesare de date și informații, descriere, clasificare, etichetare, traduceri etc.). Munca colaborativă constă în utilizarea unei platforme digitale ce poate fi accesată via computere sau telefoane mobile pentru intermedierea relațiilor dintre furnizorii de servicii (e.g. servicii de transport urban, cazare, ospitalitate, reparații sau alte servicii casnice) și beneficiarii acestora*”. Aşadar, diferența dintre cele două forme de muncă constă în faptul că în primul caz, activitățile sau serviciile sunt efectuate online, în schimb, în al doilea caz sunt avute în vedere activități sau servicii efectuate offline, pe baza cererii și a ofertei, care se întâlnesc prin intermediul unei aplicații.

[9] Ch. Fuchs, S. Sevignani, *What is Digital Labour? What is Digital Work? What's their Difference? And why do these Questions Matter for Understanding Social Media?* [Online] la https://www.triple-c.at/index.php/tripleC/article/view/461, accesat 15.10.2021.

muncă[10], posibilitatea exceptării de la anumite responsabilităţi impuse de lege, cum este cazul salariaţilor cu dizabilităţi, cărora nu mai este necesar să le asigure *„accesibilizarea la locul de muncă”*[11].

3. Riscurile psihosociale asociate muncii digitale

În schimb, efectele asupra sănătăţii lucrătorilor pot dezechilibra balanţa efectelor pozitive anterior menţionate, printre efectele nocive ale muncii digitale fiind riscurile psihosociale asociate.

Potrivit Agenţiei Europene pentru Sănătate şi Securitate în Muncă (AESSM), *„riscurile psihosociale sunt generate de conceperea, organizarea şi gestionarea precară a activităţii, precum şi de un context social necorespunzător la locul de muncă şi pot avea efecte negative pe plan psihologic, fizic sau social, precum stresul la locul de muncă, epuizarea sau depresia”*[12].

AESSM identifică şi o serie de condiţii de lucru care determină riscuri psihosociale, printre care: *„volumul excesiv de muncă; cerinţele contradictorii şi lipsa de claritate privind rolul pe care îl are de îndeplinit lucrătorul; lipsa de implicare în luarea deciziilor care afectează lucrătorul şi lipsa de influenţă asupra modului de desfăşurare a activităţii; schimbările organizatorice gestionate necorespunzător, nesiguranţa locului de muncă; comunicarea ineficientă, lipsa de sprijin din partea conducerii sau a colegilor; hărţuirea psihologică şi sexuală, violenţa din partea terţilor.*”

În opinia noastră, o parte dintre aceste condiţii de lucru care sunt de natură să genereze riscuri psihosociale sunt adesea întâlnite şi în cazul muncii digitale, respectiv: (i) volumul excesiv de muncă, (ii) comunicarea ineficientă, (iii) lipsa de sprijin din partea conducerii sau a colegilor şi (iv) hărţuirea psihologică.

Aşa cum vom detalia în secţiunea următoare aceste condiţii sunt de natură a avea efecte negative pe plan psihologic, fizic sau social asupra lucrătorilor.

3.1. Volumul excesiv de muncă al lucrătorilor digitali

În ceea ce priveşte volumul excesiv de muncă, potrivit studiului OIM privind viitorul muncii şi munca pe platforme digitale[13], un procent de 52% dintre respondenţi[14] au raportat că au lucrat în mod regulat cel puţin şase zile pe săptămână (16% la sută au lucrat regulat şase zile şi 36 % au lucrat regulat şapte zile pe săptămână). O mare parte a lucrătorilor au lucrat în timpul nopţii (43% în

[10] A. Cioriciu Ştefănescu, *Telemunca*, Revista Romana de Dreptul Muncii nr. 1 din 2009, [Online] la https://idrept.ro/?Form=reviste&Search=yes&PublicationType=22, accesat 21.10.2021.

[11] M. E. Marica, *Contracte de muncă atipice*, Editura Universul Juridic, Bucureşti, 2019, p. 313.

[12] Agenţia Europeană pentru Sănătate şi Securitate în Muncă, *Riscurile psihosociale şi stresul la locul de muncă,* [Online] la https://osha.europa.eu/ro/themes/psychosocial-risks-and-stress, accesat 20.10.2021.

[13] J. Berg (coord), *Digital labour platforms and the future of work. Towards decent work in the online world*, International Labour Office, 2018, [Online] la https://www.ilo.org/global/publications/books/WCMS_645337/lang--en/index.htm, accesat 15.10.2021, p. xvi.

[14] J. Berg (coord), *op. cit*, p. 42.

intervalul orar 22:00 - 5:00) şi seara (68% în intervalul orar 18:00 - 22:00), fie ca răspuns la disponibilitatea sarcinilor, fie din cauza altor angajamente. Aproximativ 18% dintre lucrători au raportat că au lucrat peste două ore noaptea timp de mai mult de 15 zile pe lună. Mai mult, aproximativ 44% dintre lucrători au lucrat mai mult de 10 ore pe zi până la o treime din lună (1-10 zile), iar 23% dintre aceştia au avut un program îndelungat de muncă timp de 11-30 de zile într-o lună.

În schimb, telelucrătorii, bucurându-se de componenta de flexibilitate specifică telemuncii, tind să îşi *„elasticizeze"* timpul şi să includă pe durata programului clasic de muncă sarcini din sfera personală, de cele mai multe ori cu consecinţa prelungirii orelor de terminare a programului.

Încercarea de a suplimenta veniturile, prin prestarea unor activităţi suplimentare, în cazul lucrătorilor pe platforme sau încercarea telelucrătorilor de a-şi elasticiza timpul de muncă, fără a avea o limită maximă a numărului de ore lucrate, duce la incapacitatea individului de a-şi reface capacitatea de muncă şi de a se odihni şi recrea, funcţii specifice perioadelor de repaus garantate de legislaţia muncii.

Potrivit Rezoluţiei PE Parlamentului European din 21 ianuarie 2021 conţinând recomandări adresate Comisiei privind dreptul de a se deconecta, *„numărul persoanelor din Uniune care lucrează de acasă şi care declară că au un program de lucru prelungit şi nu pot beneficia de perioadele nelucrătoare este în creştere; constată, de asemenea, că persoanele care lucrează de la distanţă în mod obişnuit sunt mai susceptibile să declare că suferă de stres profesional şi că sunt afectate de tulburări de somn, de stres şi de expunerea la lumina ecranelor digitale şi observă că alte efecte asupra sănătăţii lucrătorilor de la distanţă şi a lucrătorilor „foarte mobili" sunt durerile de cap, de ochi, oboseala, anxietate şi afecţiunile muscularo-scheletice".*

3.2. Comunicarea ineficientă şi lipsa de sprijin din partea conducerii sau a colegilor

În ceea ce priveşte comunicarea ineficientă şi lipsa de sprijin din partea conducerii sau a colegilor, acestea rezidă de cele mai multe ori în izolarea cu care se confruntă lucrătorul digital.

Potrivit unui interviu acordat de medicul psihiatru Prof. Dr. Manfred Spitzer[15], profesor de psihiatrie la Clinica Universitară din Ulm, *„ştim că forma extremă de izolare – carantina – poate duce la dereglări psihice chiar şi la persoane cu un psihic sănătos. Există studii pe termen lung care arată că, după o perioadă de carantină, oamenii se confruntă mai frecvent cu probleme cum ar fi anxietatea, insomnia sau dificultăţi în a face faţă stresului. S-a mai constatat că nu există diferenţe în acest sens între persoane tinere sau vârstnice, între bărbaţi şi femei".*

[15] Interviu, Prof. Dr. Manfred Spitzer, *Pandemie şi carantină: Singurătatea e contagioasă,* [Online] la https://www.dw.com/ro/pandemie-%C5%9Fi-carantin%C4%83-singur%C4%83tatea-e-contagioas% C4%83/a-52966096, accesat 17.10.2021.

Lipsa interacţiunii şi a sprijinului din partea colegilor poate fi un factor care să conducă la burnout[16], fenomen pe care îl vom analiza în secţiunile următoare.

Efecte ale izolării au loc şi în plan social. Astfel, izolarea[17] este asociată cu lipsa accesului la schimbul informal de informaţii care are loc la birou, dar şi cu crearea unor bariere în carieră, deoarece mulţi lucrători la distanţă nu sunt *„văzuţi"* de managerii lor[18].

De asemenea, izolarea duce şi la lipsa contactului direct cu clienţii, ce se concretizează în faptul că un lucrător pe platformă din trei (32%) a raportat că are o experienţă de neplată pentru munca sa prin intermediul platformelor online.

3.3. Hărţuirea psihologică

În ceea ce priveşte hărţuirea psihologică, plecând de la definiţia oferită de legislaţia internă, şi anume de O.G. nr. 137/2000[19] şi de Legea nr. 202/2002[20] putem

[16] Ch. Aumayr-Pintar, C. Cerf, A. Parent-Thirion, *Burnout in the workplace: A review of data and policy responses in the EU*, European Foundation for the Improvement of Living and Working Conditions, Luxemburg, 2018, p. 16, [Online] la https:// www.eurofound.europa.eu/publications/report/2018/burnout-in-the-workplace-a-review-of-data-and-policy-responses-in-the-eu, accesat 22.10.2021. Un factor recurent în apariția burnoutului este absența sprijinului social din partea colegilor.

[17] *Idem*, p. 17. Potrivit studiilor realizate în Marea Britanie și Bulgaria, munca în echipă reduce nivelul de burnout. În schimb, lipsa oportunităților de învățare și dezvoltare la locul de muncă a dovedit creșterea probabilității epuizării. Pe de altă parte, un alt factor determinant pentru burnout este rolul managementului și al conducerii, lipsa de sprijin din partea managementului crescând riscul de epuizare, pe când mentoratul, aprecierea și încrederea din conducerii are un impact pozitiv în atenuarea epuizării și menținerea sau restabilirea motivației la locul de muncă.

[18] Ch. Welz, F. Wolf, *Telework in the European Union*, European Foundation for the Improvement of Living and Working Conditions, 2010, p. 20, [Online] la https://www.eurofound.europa.eu/publications/report/2010/telework-in-the-european-union, accesat 23.10.2021.

[19] Art. 2 alin. *„(5[1]) Constituie hărțuire morală la locul de muncă și se sancționează disciplinar, contravențional sau penal, după caz, orice comportament exercitat cu privire la un angajat de către un alt angajat care este superiorul său ierarhic, de către un subaltern și/sau de către un angajat comparabil din punct de vedere ierarhic, în legătură cu raporturile de muncă, care să aibă drept scop sau efect o deteriorare a condițiilor de muncă prin lezarea drepturilor sau demnității angajatului, prin afectarea sănătății sale fizice sau mentale ori prin compromiterea viitorului profesional al acestuia, comportament manifestat în oricare dintre următoarele forme: a) conduită ostilă sau nedorită; b) comentarii verbale; c) acțiuni sau gesturi. (5[2]) Constituie hărțuire morală la locul de muncă orice comportament care, prin caracterul său sistematic, poate aduce atingere demnității, integrității fizice ori mentale a unui angajat sau grup de angajați, punând în pericol munca lor sau degradând climatul de lucru. În înțelesul prezentei legi, stresul și epuizarea fizică intră sub incidența hărțuirii morale la locul de muncă".*

[20] Art. 4 lit. d[1] *„prin hărţuire psihologică se înţelege orice comportament necorespunzător care are loc într-o perioadă, este repetitiv sau sistematic şi implică un comportament fizic, limbaj oral sau scris, gesturi sau alte acte intenţionate şi care ar putea afecta personalitatea, demnitatea sau integritatea fizică ori psihologică a unei* persoane".

concluziona că în cazul muncii digitale, lucrătorii digitali se pot confrunta cu mai multe forme de hărţuire morală şi/sau psihologică, dat fiind că aceştia sunt supuşi stresului şi epuizării fizice, aşa cum vom detalia în secţiunile următoare.

În primul rând, în cazul lucrătorilor pe platforme, consecinţele negative la nivel psihologic sunt cauzate chiar de natura muncii prestate de aceştia, un exemplu concret fiind cel al lucrătorilor care moderează conţinutul site-urilor web bazate pe conţinut generat de utilizator şi elimină conţinutul semnalat ca fiind necorespunzător, pentru ca utilizatorului să-i fie prezentată o imagine relativ curată a respectivului site. Astfel, lucrătorii în cauză sunt expuşi constant la conţinut neadecvat, ce poate avea efecte psihologice pe termen lung, cum ar fi insomnie, coşmaruri, anxietate sau halucinaţii.

Pe de altă parte, majoritatea sarcinilor lucrătorilor pe platforme o reprezintă microsarcini simple şi repetitive ce nu coincid cu nivelul ridicat de educaţie al lucrătorilor, care este de natură a genera consecinţele negative pe plan psihologic menţionate anterior.

Nu în ultimul rând unul dintre riscurile sociale generate de munca digitală îl constituie tendinţele de exploatare ale platformelor pentru a crea o experienţă superioară pentru clienţii lor, în detrimentul lucrătorilor[21], care se materializează într-un climat de lucru stresant, de natură a atrage epuizarea fizică şi psihică a lucrătorului.

Cu titlu de exemplu menţionăm cazul Uber, unde, dacă un pasager uită un bun în maşină în timpul cursei, şoferul îl va returna în timpul său liber, fără a fi plătit. Aceeaşi platformă oferă pasagerilor opţiunea de a plăti mai puţin dacă folosesc o călătorie comună cu alţi pasageri decât dacă folosesc o călătorie standard. Deşi pasagerii sunt avantajaţi, plătind mai puţin pentru aceeaşi cursă, acest lucru este în detrimentul lucrătorilor, care trebuie să ridice mai mulţi pasageri din diferite puncte, ceea ce duce la curse întârziate şi, deci la o experienţă mai puţin calitativă pentru pasageri. Astfel, aceştia vor avea motive să acorde şoferilor calificări slabe, lucrătorul fiind dezavantajat în detrimentul asigurării confortului pasagerului.

4. Efectele negative ale muncii digitale asupra lucrătorului

Toate aceste condiţii de lucru de natură să creeze riscuri psihosociale au efecte atât asupra sănătăţii fizice, cât şi a celei psihice a lucrătorilor.

4.1. Efectele asupra sănătăţii fizice

Printre efectele asupra sănătăţii fizice cauzate de munca digitală se numără dureri de gât şi tendon la încheieturi şi degete[22] cauzate de munca pe dispozitive digitale, dureri fizice cauzate de lipsa unui spaţiu de lucru fizic adecvat şi de sedentarismul prelungit, dar şi probleme digestive ca urmare a reducerii activităţii

[21] *Ibidem.*

[22] A se vedea J. Messenger, O. Vargas Llave, L. Gschwind, S. Boehmer, G. Vermeylen, M. Wilkens, *op. cit.*, p. 34.

fizice generale şi a exerciţiilor fizice, combinate cu un aport global crescut de alimente[23].

La rândul său, stresul resimţit de lucrătorii digitali menţionat în secţiunea anterioară poate cauza boli cardiovasculare şi tulburări musculo-scheletice, dar şi oboseală continuă, dureri de cap, lipsa de concentrare, lipsa de energie şi hipertensiune arterială, hipercolesterolemie, diabet de tip 2, boli coronariene, tulburări cardiovasculare, dureri musculo-scheletice, oboseală prelungită, dureri de cap, probleme gastro-intestinale, probleme respiratorii, leziuni severe şi mortalitate sub vârsta de 45 de ani[24].

4.2. Efectele asupra sănătăţii psihice

Potrivit Rezoluţiei PE Rezoluţia Parlamentului European din 21 ianuarie 2021 conţinând recomandări adresate Comisiei privind dreptul de a se deconecta, *„utilizarea excesivă a dispozitivelor tehnologice poate agrava fenomene precum izolarea, dependenţa de tehnologie, privarea de somn, epuizarea emoţională, anxietatea şi oboseala extremă; întrucât, potrivit OMS, la nivel mondial peste 300 de milioane de persoane suferă de depresie şi de tulburări de sănătate mentală comune legate de muncă şi 38,2 % din populaţia Uniunii suferă de o tulburare de sănătate mentală în fiecare an”.*

În ceea ce priveşte efectele asupra sănătăţii psihice, cel mai important efect al muncii digitale este burnoutul, definit de Organizaţia Mondială a Sănătăţii ca fiind un sindrom conceptualizat ca rezultat al stresului cronic la locul de muncă care nu a fost gestionat cu succes, fiind caracterizat prin trei dimensiuni: epuizarea energiei, creşterea distanţării mentale faţă de locul de muncă sau sentimentele de negativism sau cinism legate de locul de muncă şi eficacitate profesională redusă.

Burnoutul[25] are consecinţe majore pe termen lung asupra vieţii lucrătorilor. Studiile arată că lucrătorii care se confruntă cu un nivel ridicat de epuizare emoţională: au renunţat relativ des la a mai presta muncă, în decurs de doi ani (4,1%, comparativ cu 2,3% dintre cei care nu suferiseră de epuizare emoţională); erau, de asemenea, mai predispuşi să se afle în concediu medical pe perioade mai lungi decât ceilalţi lucrători; consideră schimbarea locului de muncă o modalitate de a scăpa de situaţia lor stresantă; îşi exprimă, de asemenea, relativ des dorinţa de a-şi reduce programul de lucru, dar de fapt nu o fac mai des decât persoanele care nu se confruntă cu epuizarea.

---

[23] X. Yijing, B.Becerik-Gerber, L. Gale, S.C. Roll, *Impacts of Working From Home During COVID-19 Pandemic on Physical and Mental Well-Being of Office Workstation Users*, [Online] la https://journals.lww.com/joem/fulltext/2021/03000/impacts_of_working_from_home_during_covid_19.2.aspx, accesat 15.10.2021.

[24] Ch. Aumayr-Pintar, C. Cerf, A. Parent-Thirion, *op. cit.*, p. 12.

[25] *Idem,* p. 3. Prima referire la burnout îi este atribuită lui Freudenberger, care, plecând de la definiția verbului „*to burn out*” („*a eșua, a se uza sau a deveni epuizat ca urmare a solicitării excesive de energie, putere sau resurse*”), afirma că exact același lucru se întâmplă cu un lucrător care ajunge la stadiul de burnout, devenind ineficace. Corelația ridicată dintre epuizare, depresie și anxietate este explicată de Toker și colab. (2005).

Aşadar, burnoutul, care reprezintă unul dintre efectele asupra sănătăţii psihice a lucrătorilor digitali, are la rândul său efecte asupra sănătăţii fizice a acestora, dar şi asupra vieţii lor sociale.

4.3. Efecte sociale

În ceea ce priveşte efectele sociale, cel mai cunoscut efect al muncii digitale îl constituie eliminarea limitei dintre viaţa profesională şi cea personală, care poate culmina cu conflicte ale lucrătorului cu familia şi neglijarea sarcinilor casnice[26]. Studii efectuate în Irlanda arată că lucrătorii care au în grijă copiii de vârstă preşcolară întâmpină cele mai mari dificultăţi în concilierea vieţii profesionale cu viaţa de familie[27].

Acest conflict dintre viaţa personală şi viaţa profesională poate da naştere unui stres continuu resimţit de lucrător, care, la rândul său poate cauza efectele fizice sau psihologice descrise mai sus.

Apoi, ca urmare a problemelor de sănătate ale lucrătorului, acesta absentează de la locul de muncă, ceea ce implică o serie de costuri pentru angajatori şi pentru sistemele de securitate socială, cum ar fi sistemele de invaliditate, incapacitate şi indemnizaţii de şomaj.

5. Măsuri adoptate la nivel internaţional pentru combaterea riscurilor psihosociale asociate muncii digitale. Dreptul la deconectare

Riscurile psihosociale şi efectele negative ale muncii digitale sunt deja cunoscute la nivel internaţional, în acest sens fiind adoptate măsuri pentru combaterea şi prevenirea acestora, atât de către state, prin adoptarea unor norme speciale, cât şi de angajatori, prin adoptarea unor politici interne.

5.1. Măsuri adoptate la nivel legislativ, dar şi la nivel de angajatori

O primă măsură luată de autorităţi o reprezintă monitorizarea fenomenului burnout. De exemplu, în Olanda, Inspectoratul Olandez al Muncii monitorizează un eşantion de aproximativ 2.000 de organizaţii cu privire la anumite condiţii de muncă, în 2007, în prim-plan fiind stresul legat de muncă. De asemenea, Inspectoratul bulgar de muncă, în cadrul inspecţiilor desfăşurate, a analizat dacă salariaţii angajaţii lucrează cu termene limitate strânse, dacă au experimentat presiuni de timp, agresiune sau hărţuire sau lipsă de autonomie la locul de muncă[28].

O altă măsură este desfăşurarea unor campanii de informare derulate de autorităţi. Un exemplu este cel al Estoniei, unde Inspectoratul muncii a dezvoltat o

[26] J. Messenger, O. Vargas Llave, L. Gschwind, S. Boehmer, G. Vermeylen, M. Wilkens, *op. cit.*, p. 36.

[27] A. Broughton, *Work-related stress*, European Foundation for the Improvement of Living and Working Conditions, Dublin, 2010, p. 14, [Online] la https://www.eurofound.europa.eu/publications/report/2010/work-related-stress, accesat 26.10.2021.

[28] *Ibidem.*

pagină web dedicată stresului legat de muncă, care include un instrument de auto-analiză pentru companii pentru măsurarea stresului legat de muncă. De asemenea, aceeaşi autoritate a desfăşurat campanii sociale privind gestionarea stresului profesional, bazat pe bunele practici utilizate de companii la nivel naţional[29]. În Luxemburg există un centru de resurse pentru prevenirea şi gestionarea stresului cronic pentru a oferi îndrumări şi sprijin pentru prevenirea epuizării şi asistenţă pentru cei care suferă de epuizare[30].

După monitorizare şi informarea actorilor implicaţi despre stresul la locul de muncă, atât angajatorii, cât şi autorităţile au luat măsuri de diminuare a stresului la locul de muncă. În anumite state autorităţile au adoptat măsuri în sensul facilitării obţinerii unor perioade suplimentare de repaus, în anumite condiţii excepţionale. De exemplu, în Belgia, începând din 2017 legea acordă salariaţilor posibilitatea de a dona colegilor zile de concediu către un alt salariat, pentru a facilita echilibrul între viaţa profesională şi viaţa personală a angajaţilor şi pentru a reduce epuizarea[31]. Acelaşi lucru este posibil şi în Franţa, însă doar pentru salariaţii care au un copil bolnav, dar şi în anumite societăţi din Italia[32].

La nivel de angajatori, au fost adoptate o serie de măsuri care să sporească bunăstarea lucrătorilor, după cum urmează: Olho-Technik Czech asigură salariaţilor vitamine şi vouchere la centre de wellness, organizând totodată examinări medicale la locul de muncă; MSFT Microsoft Portugalia a oferit asistenţă psihologică gratuită pentru lucrători, masaj gratuit în timpul muncii, cofinanţarea unui club de sănătate şi a unui club sportiv (extins la membrii familiei) şi furnizarea de spaţii de fitness în cadrul spaţiilor de birouri; Slovnaft şi-a înfiinţat propria unitate psihologică pentru a ajuta la prevenirea stresului la locul de muncă, a accidentelor la locul de muncă şi a bolilor profesionale[33].

5.2. Dreptul la deconectare

O altă măsură adoptată atât la nivel de angajatori, cât şi la nivel de autorităţi a fost reglementarea dreptului la deconectare. Orange a consacrat în Franţa, la nivel de contract colectiv de muncă în anul 2016 dreptul la deconectare. În Germania, în 2012, Volkswagen a impus „îngheţarea" e-mailurilor în afara orelor de program, setând serverele interne să se abţină de la trimiterea de e-mailuri în conturi individuale între orele 18.15 şi 07.00[34]. În 2014, societatea Daimler a introdus un

[29] Ch. Aumayr-Pintar, C. Cerf, A. Parent-Thirion, *op. cit.*, p. 27.

[30] *Ibidem.*

[31] Ch. Aumayr-Pintar, C. Cerf, A. Parent-Thirion, *op. cit.*, p. 24.

[32] O. Vargas Llave; S. Boehmer, *Policies to improve work– life balance,* European Foundation for the Improvement of Living and Working Conditions, 2015, [Online] la https://www.eurofound.europa.eu/publications/report/2015/eu-member-states/policies-to-improve-work-life-balance, accesat 22.10.2021.

[33] A. Broughton, *Work-related stress, op. cit.*

[34] European Foundation for the Improvement of Living and Working Conditions, *Right to disconnect*, [Online] la https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/right-to-disconnect, accesat 24.10.2021.

software numit „Mail on Holiday" pe care angajaţii săi îl puteau folosi pentru a şterge automat e-mailurile primite în timp ce erau în vacanţă[35]. În Spania, contractul colectiv al companiei încheiat la compania de asigurări AXA în iulie 2017, care stabilea dreptul angajaţilor de a-şi opri telefoanele în afara programului de lucru. Lidl din Belgia şi Luxemburg a implementat un software prin care e-mailurile interne care sunt trimise după ora 18:00 nu vor fi livrate destinatarului intern până la 7:00 a doua zi.

Aşa cum s-a reţinut în Rezoluţia Parlamentului European din 21 ianuarie 2021 conţinând recomandări adresate Comisiei privind dreptul de a se deconecta utilizarea instrumentelor digitale în scopuri profesionale *„a dus la apariţia unei culturi de a fi „conectat în permanenţă" „mereu online" sau „mereu de serviciu", care poate influenţa negativ drepturile fundamentale ale lucrătorilor şi condiţiile de muncă echitabile, inclusiv remunerarea echitabilă, limitarea timpului de lucru, echilibrul dintre viaţa profesională şi cea privată, sănătatea fizică şi mentală, securitatea în muncă şi starea de bine, precum şi egalitatea dintre bărbaţi şi femei, din cauza impactului disproporţionat asupra lucrătorilor cu responsabilităţi de îngrijire, care tind să fie femei".*

În acest sens, Parlamentul European propune consacrarea prin intermediul unei directive a dreptului la deconectare, propunând ca definiţie *„a se deconecta" înseamnă a nu se implica în activităţi sau comunicări legate de activitatea profesională prin intermediul unor instrumente digitale, direct sau indirect, în afara timpului de lucru".*

În viziunea Parlamentului European, statele membre ar urma să se asigure că angajatorii iau măsurile necesare pentru a le oferi lucrătorilor mijloacele necesare pentru a-şi exercita dreptul de a se deconecta şi că aceştia instituie un sistem obiectiv, fiabil şi accesibil care să permită măsurarea duratei timpului de lucru zilnic al fiecărui lucrător. Printre condiţiile minime de lucru ce ar trebui implementate la nivelul statelor membre se numără: modalităţile practice de închidere a instrumentelor digitale folosite în scopuri profesionale, sistemul de măsurare a timpului de lucru, evaluări în materie de sănătate şi securitate, inclusiv evaluări ale riscurilor psihosociale, legate de dreptul de a se deconecta, criteriile pe baza cărora se acordă angajatorilor orice derogare[36] de la obligaţia de a pune în aplicare dreptul lucrătorilor de a se deconecta, criteriile de stabilire a modului în care trebuie calculată compensaţia pentru munca prestată în afara timpului de lucru, măsurile de sensibilizare, inclusiv formare la locul de muncă, care urmează să fie luate de către angajatori în ceea ce priveşte condiţiile de muncă menţionate la prezentul alineat.

[35] M. Gibson, *Here's a Radical Way to End Vacation Email Overload*, [Online] la https://time.com/3116424/daimler-vacation-email-out-of-office/, accesat 23.10.2021.

[36] Orice derogare ar urma să se acorde numai în circumstanţe excepţionale, cum ar fi cazurile de forţă majoră sau alte situaţii de urgenţă, şi cu condiţia ca angajatorul să ofere fiecărui lucrător în cauză, în scris, motive care să justifice necesitatea derogării, de fiecare dată când se invocă derogarea.

De asemenea, potrivit propunerii de directivă, statele membre ar urma să se asigure că lucrătorii cărora le-a fost încălcat dreptul de a se deconecta au acces la mecanisme rapide, eficace şi imparţiale de soluţionare a litigiilor şi au dreptul la repararea prejudiciului în cazul încălcării drepturilor lor care decurg din prezenta directivă.

Deşi la acest moment nu există încă adoptată o astfel de directivă, o serie de state membre au adoptat măsuri legislative pentru a garanta acest drept, măsuri similare fiind luate şi la nivelul altor state din afara Uniunii Europene.

În Franţa, potrivit art. 2242-8 pct. 7 din Codul Muncii, negocierile anuale privind egalitatea profesională între femei şi bărbaţi şi calitatea vieţii la locul de muncă au în vedere procedurile pentru exercitarea deplină de către salariat a dreptului său la deconectare şi stabilirea de către întreprindere a mecanismelor de reglementare pentru utilizarea instrumentelor digitale, astfel încât să fie asigurată respectarea timpilor de odihnă şi de concediu, precum şi a vieţii personale şi de familie.

În Spania, potrivit art. 88 din Legea pentru Protecţia Datelor[37], atât lucrătorii din mediul public, cât şi cei din mediul privat au dreptul la deconectare digitală astfel încât să le fie garantat, pe lângă timpul de muncă, şi respectarea timpului lor de odihnă, concediul, precum şi intimitatea lor personală şi familială. În acest sens, angajatorul, după audierea reprezentanţilor lucrătorilor, va întocmi o politică internă în care va defini modalităţile de exercitare a dreptului la deconectare şi acţiunile de formare şi conştientizare cu privire la o utilizare rezonabilă a instrumentelor digitale.

În Italia, art. 19 din Legea nr. 81/2017[38] consacră dreptul la deconectare doar în cazul prestării *„muncii inteligente”*, care este o modalitate de prestare a muncii stabilită prin acord al părţilor, ce implică organizare pe faze, cicluri şi obiective, fără constrângeri precise de timp sau loc de muncă, cu posibilitatea de utilizare a instrumentelor digitale pentru prestarea muncii. Astfel, munca este prestată parţial în incinta întreprinderii şi parţial în exterior, fără un loc de muncă fix şi numai în limitele duratei maxime timpului de muncă. Acordul părţilor pentru prestarea muncii inteligente trebuie să conţină perioadele de repaus al lucrătorului, precum şi măsuri tehnice şi organizatorice necesare pentru a asigura deconectarea lucrătorului de la instrumente de lucru.

Similar legislaţiei din Italia, şi în Chile[39] dreptul la deconectare este consacrat doar pentru o categorie determinată de lucrători. Potrivit legislaţiei acestei ţări, în

[37] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, [Online] la https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673, accesat 23.10.2021.

[38] Legge 22 maggio 2017, n. 81 Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato, [Online] la https://www.gazzettaufficiale.it/eli/%20id/2017/06/13/17G00096/sg, accesat 21.10.2021.

[39] Ley 21220 modifica el código del trabajo en materia de trabajo a distancia, [Online] la https://www.leychile.cl/Navegar?idNorma=1143741, accesat 21.10.2021.

cazul lucrătorilor la distanţă care îşi stabilesc singuri programul de muncă şi în cazul telelucrătorilor excluşi de la limitarea programului de lucru, angajatorul trebuie să respecte dreptul acestora la deconectare, garantându-le un timpul în care nu vor fi obligaţi să răspundă la comunicări, ordine sau alte cerinţe ale angajatorului.

Legislaţie din Chile merge însă mai departe decât legislaţia din Italia şi prevede că timpul de deconectare trebuie să fie de cel puţin douăsprezece ore continue într-o perioadă de douăzeci şi patru de ore. De asemenea, în niciun caz angajatorul nu poate transmite comunicări, ordine sau alte cerinţe în timpul zilelor de concediu ale lucrătorilor.

În mod similar în Argentina[40], potrivit art. 5 din Legea 27.555 privind telemunca, telelucrătorul are dreptul de a se deconecta de la dispozitivele digitale şi/sau tehnologiile informaţiei şi comunicaţiilor, în afara programului său de lucru şi în perioadele de concediu. Legea prevede expres că telelucrătorul nu poate fi sancţionat pentru exercitarea acestui drept.

În Slovacia, potrivit modificărilor Codului Muncii care au intrat în vigoare de la 1 martie 2021[41], salariatul care desfăşoară activităţi casnice şi telelucrătorul au dreptul la repaus zilnic şi săptămânal neîntrerupt, cu excepţia cazului în care aceştia prestează muncă on-call sau muncă suplimentară. Astfel, angajatorul nu poate considera că refuzul salariatului de a presta munca în aceste perioade reprezintă o încălcare a obligaţiilor contractuale.

În schimb, în Belgia, potrivit Legii privind întărirea creşterii economice şi coeziunii sociale, pentru a asigura respectarea perioadelor de repaus ale lucrătorilor şi pentru a menţine echilibrul dintre muncă şi viaţa privată, angajatorul organizează consultări în cadrul Comitetului pentru Prevenire şi Protecţie în Muncă cu privire la deconectarea de la locul de muncă şi utilizarea mijloacelor digitale de comunicare[42]. Aşa cum s-a arătat în literatura de specialitate[43] *„angajaţii din Belgia au dreptul de a discuta cu angajatorii lor chestiunile referitoare la deconectare, dar nu au dreptul la deconectare în sensul strict al termenului. Angajatorul poate să adopte politici de deconectare după ce se consultă cu comitetul, dar nu este obligat să facă asta”.*

[40] Régimen legal del contrato de teletrabajo, Ley 27555, [Online] la https:// www.boletinoficial.gob.ar/detalleAviso/primera/233626/20200814, accesat 21.10.2021.

[41] Zákonník Práce [Online] la https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/ 311/ 20210301.html#paragraf-52.odsek-10, accesat 21.10.2021.

[42] Loi relative au renforcement de la croissance économique et de la cohésion sociale, [Online] la https://www.ejustice.just.fgov.be/ cgi_loi/change_lg.pl?language=fr&la= F&table_name=loi&cn=2018032601, accesat 21.10.2021.

[43] L.Dima, A. Högback, *Legiferarea dreptului la deconectare,* Friedrich-Ebert-Stiftung, România, 2020, [Online] la http://library.fes.de/pdf-files/bueros/bukarest/17026.pdf, accesat 21.10.2021.

Un exemplu similar este cel al Irlandei, cel mai recent stat care a consacrat dreptul la deconectare, în acest caz însă, prin intermediul unui Cod de Practică[44] ce stabileşte îndrumări şi bune practici pentru angajatori şi angajaţi în ceea ce priveşte respectarea legislaţiei muncii.

Potrivit acestui Cod, dreptul la deconectare implică trei aspecte principale: (i) dreptul unui lucrător de a nu presta în mod regulat muncă în afara programului normal de lucru; (ii) dreptul unui lucrător de a nu fi penalizat pentru refuzul de a presta munca în afara programului normal de lucru şi (iii) obligaţia de a respecta dreptul altei persoane la deconectare (de exemplu, obligaţia de a nu trimite e-mailuri sau de a nu telefona în mod obişnuit în afara programului normal de lucru).

În acest sens, sunt prevăzute o serie de obligaţii atât pentru angajator, cât şi pentru lucrător. În ceea ce priveşte angajatorul, acesta are obligaţia de a informa lucrătorii cu privire la durata timpului de muncă, de a se asigura că aceştia beneficiază de perioadele de repaus, de a asigura un mediu de lucru sigur şi de a nu sancţiona niciun lucrător care îşi exercită drepturile prevăzute de lege în materie de sănătate şi securitate în muncă. Pe de altă parte, lucrătorii au obligaţia de a se asigura că îşi gestionează în mod corespunzător timpul de muncă, de a respecta legislaţia în materie de sănătate şi securitate în muncă, de a înregistra timpul de lucru prin intermediul mecanismelor puse la dispoziţie de angajator, de a respecta dreptul colegilor la deconectare, de a-şi notifica în scris angajatorul cu privire la orice perioadă de repaus la care sunt îndreptăţiţi şi de care nu pot beneficia, de a avea grijă de bunăstarea lor legată de muncă şi de a lua orice măsuri de remediere, dacă este necesar.

De asemenea, Codul promovează o serie de reguli în materie de comunicare: indicarea programului normal de lucru al salariatului în cadrul semnăturii ataşate emailului, crearea unor răspunsuri automate de tip „out of office" şi la încheierea programului de muncă, nu doar pe durata concediilor.

6. Propuneri de lege ferenda

Având în vedere efectele negative psihosociale pe care munca digitală le are asupra lucrătorilor, considerăm utilă legiferarea unor măsuri care să prevină şi să combată aceste efecte.

În primul rând, este necesară modificarea legislaţiei naţionale şi adaptarea acesteia la realităţile economice şi sociale. Un prim pas ar fi reglementarea muncii digitale, care în ceea ce ne priveşte, poate fi definită ca acea formă de prestare a muncii prin care lucrătorul îşi îndeplineşte atribuţiile specifice funcţiei, ocupaţiei sau meseriei pe care o deţine folosindu-se preponderent de instrumente digitale.

Având în vedere specificul acestui tip de muncă, precum şi riscurile psihosociale inerente, se impune totodată reglementarea unor măsuri de combatere a acestor riscuri. În opinia noastră acestea ar trebui să aibă în vedere condiţiile de

[44] Code of practice for employers and employees on the right to disconnect, [Online] la https://workplacerelations.ie/wrc/en/what_you_should_know/codes_practice/code-of-practice-for-employers-and-employees-on-the-right-to-disconnect.pdf, accesat 21.10.2021.

lucru care sunt caracteristice muncii virtuale şi care, aşa cum a reţinut AESSM sunt asociate riscurilor psihosociale.

În ceea ce priveşte combaterea volumului excesiv de muncă al lucrătorilor digitali, considerăm utilă instituirea obligaţiei angajatorilor de a adopta proceduri care să asigure respectarea duratei maxime a timpului de lucru. Aşa cum s-a arătat şi prin Rezoluţiei Parlamentului European din 21 ianuarie 2021 conţinând recomandări adresate Comisiei privind dreptul de a se deconecta *„înregistrarea eficace a timpului de lucru poate contribui la respectarea timpului de lucru stabilit prin contract”*[45].

În acest sens, recomandăm promovarea unei culturi care să permită lucrătorului deconectarea de la mediul de lucru în afara perioadei de lucru, materializată prin organizarea muncii şi a volumului de muncă ţinând cont de numărul personalului disponibil, consacrarea unor obiective realizabile fără o conexiune a lucrătorului în afara programului de muncă, lipsa de sancţiune a lucrătorilor care nu pot fi contactaţi în afara programului de muncă.

Totodată, deşi criticat în practică[46], un instrument util pentru respectarea duratei timpului de muncă, dar şi pentru reducerea stresului la locul de muncă, şi implicit al combaterii hărţuirii psihologice o constituie reglementarea dreptului la deconectare.

Similar prevederilor Codului de practică din Irlanda, considerăm util ca prin reglementarea dreptul la deconectare, să se încurajeze atât respectarea acestui drept, dar să se ţină cont şi de flexibilitatea necesară pentru desfăşurarea anumitor activităţi, astfel încât să nu instituie restricţii ale modelelor de comunicare şi să se permită contactarea lucrătorilor în afara programului de lucru, cu titlu ocazional şi doar justificat de motive obiective.

---

[45] Rezoluția Parlamentului European din 21 ianuarie 2021 conținând recomandări adresate Comisiei privind dreptul de a se deconecta (2019/2181(INL)), [Online] la https://www.europarl.europa.eu/doceo/document/TA-9-2021-01-21_RO.html#sdocta7, accesat 20.10.2021.

[46] S. Glaveski, *Why the right to disconnect is a bad idea*, [Online] la https://www.thehrdirector.com/features/future-of-work/why-the-right-to-disconnect-is-a-bad-idea/, accesat 27.10.2021. După consacrarea legislativă a acestui drept și punerea lui în practică, au fost însă identificate și o serie de dezavantaje ale acestui drept. Lucrătorii susțin că legislația nu poate schimba modul de desfășurare a businessurilor internaționale, care implică fusuri orare diferite, dar și un grad ridicat de competitivitate între salariați, deci implică nevoia de prestare a muncii și „după ora 18:00”. În acest sens, se propune o modificare a modalității de prestare a muncii, respectiv o trecere la o „comunicare asincronă”, caracterizată de sintagma *„Voi presta munca atunci când îmi convine*”, ceea ce se materializează în perioade de timp neîntrerupte în care lucrătorii pot efectua presta munca într-o stare de concentrare maximă, ceea ce se traduce prin productivitate crescută. Autorul articolului atrage totodată atenția asupra activităților neimportante care consumă foarte mult din timpul lucrătorului (utilizarea ședințelor, a emailurilor), când există metode mult mai eficiente pentru a organiza activitatea lucrătorilor, cum este cazul aplicațiilor de organizare a proiectelor.

De asemenea, reglementările ar trebui să țină cont de cazul lucrătorilor care lucrează în multinaţionale şi, deci care ar putea fi contactaţi de colegi care lucrează pe alte fusuri orare, în acest caz fiind necesară adoptarea unor reguli clare cu privire la exercitarea dreptului la deconectare şi, implicit la perioada de timp în care lucrătorul ar trebui să răspundă comunicărilor în acest caz.

O altă măsură pentru combaterea fenomenului hărţuirii psihologice o constituie obligarea angajatorilor de a adopta proceduri de training atât pentru lucrători, cât şi pentru manageri cu privire la caracteristicile muncii digitale, riscurile asociate şi potenţialele efecte negative. Pe de o parte, s-ar creşte gradul de încredere al managerilor în lucrătorii digitali, s-at facilita procesul de comunicare dintre aceştia, rezolvându-se inclusiv problema izolării lucrătorului digital.

Totodată, actorii implicaţi ar trebui să beneficieze de instruire cu privire la modul de respectare a regulilor privind timpul de lucru şi a regulilor de muncă specifice muncii digitale, inclusiv cu privire la modul de utilizare a instrumentelor digitale, dar şi a riscurilor de a fi conectaţi excesiv.

Nu în ultimul rând, având în vedere efectele asupra sănătăţii psihice a lucrătorilor, considerăm necesară adoptarea de urgenţă a unor măsuri de combatere a stresului şi burnoutului la locul de muncă.

În primul rând, se impune recunoaşterea burnoutului ca boală profesională[47], cu consecinţa imediată a monitorizării fenomenului la nivel naţional. Această monitorizare ar permite autorităţilor în materie să contureze unele strategii pentru prevenirea stresului la locul de muncă şi, implicit a burnoutului.

Menţionăm că, la acest moment, potrivit rezultatelor cercetării noastre, există o pagină web dedicată burnoutului[48], unde există posibilitatea de testare a nivelului de burnout resimţit, sunt prezentate articole de specialitate în materie şi se acordă consiliere online, acesta fiind un proiect finanţat prin Programul Operaţional Capital Uman 2014 – 2020 / Axa Prioritară 3: Locuri de muncă pentru toţi / POCU/82 „România Start Up Plus" .

De asemenea, ţinând cont de rezultatele acestei monitorizări, propunem legiferarea obligaţiei angajatorului de a oferi lucrătorului o serie de beneficii pentru a preveni şi combate stresul la locul de muncă şi burnoutul, cum se întâmplă deja la nivel european.

Vidul legislativ actual şi lipsa oricăror iniţiative cu privire la munca digitală echivalează, în opinia noastră, cu îngrădirea dreptului la muncă pentru lucrătorii digitali, atât timp cât aceştia sunt expuşi unor riscuri ridicate în cazul prestării acestei forme de muncă. Se impune, aşadar, iniţierea cât mai rapidă a unor proceduri şi adoptarea unor măsuri în consecinţă, pentru a răspunde nevoilor societăţii de astăzi pentru care legislaţia tradiţională nu mai este suficientă.

Aşa cum spunea A. Basilescu, *„Munca este o condiție a vieții. O suspendare, fie şi parţială a muncii, paralizează organismul social şi periclitează viaţa indivizilor,*

[47] În anumite țări din Europa legislația are în vedere reglementarea burnoutului ca boală profesională (e.g. Italia, Letonia, Olanda, Bulgaria doar în anumite sectoare de activitate). A se vedea Ch. Aumayr-Pintar, C. Cerf, A. Parent-Thirion, *op. cit.,* p. 9.

[48] A se vedea [Online] https://burnouthub.ro/, accesat 28.10.2021.

iar încetarea ei totală, fie şi numai o săptămână, ar constitui o imensă catastrofă, asemănătoare cu cele inventate de romancieri pentru a descrie sfârşitul lumii. Inactivitatea este clar sinonimă cu moartea"[49].

Referinţe

Aumayr-Pintar Ch., Cerf C., Parent-Thirion A., *Burnout in the workplace: A review of data and policy responses in the EU*, European Foundation for the Improvement of Living and Working Conditions, Luxemburg, 2018

Berg J. (coord), *Digital labour platforms and the future of work. Towards decent work in the online world*, International Labour Office, 2018

Broughton A., *Work-related stress*, European Foundation for the Improvement of Living and Working Conditions, Dublin, 2010

Ciobiciu Ştefănescu A., *Telemunca*, Revista Romana de Dreptul Muncii nr. 1 din 2009

Dima L., Högback A., *Legiferarea dreptului la deconectare*, Friedrich-Ebert-Stiftung

European Foundation for the Improvement of Living and Working Conditions, *Right to disconnect*

Fuchs Ch., Sevignani S., *What is Digital Labour? What is Digital Work? What's their Difference? And why do these Questions Matter for Understanding Social Media?*

Gibson M., *Here's a Radical Way to End Vacation Email Overload*

Ilie G., Vlăsceanu A-M., *Poate legislaţia muncii să ţină pasul cu noua realitate economică?*

Mandl I., Curtarelli M., Riso S., Vargas O., Gerogiannis E., *New forms of employment*, European Foundation for the Improvement of Living and Working Conditions, Luxemburg, 2015

Marica M.E., *Contracte de muncă atipice*, Editura Universul Juridic, Bucureşti, 2019

Organisation for Economic Co-operation and Development, *A roadmap toward a common framework for measuring the Digital Economy*, Arabia Saudită, 2020

Spitzer M., *Pandemie şi carantină: Singurătatea e contagioasă*

Ştefănescu I.T., *Tratat teoretic şi practic de drept al muncii*, Universul Juridic, Bucureşti, 2014

Vargas Llave O., Boehmer S., *Policies to improve work-life balance*, European Foundation for the Improvement of Living and Working Conditions, 2015

Welz Ch., Wolf F., *Telework in the European Union*, European Foundation for the Improvement of Living and Working Conditions, 2010

Yijing X., Becerik-Gerber B., Gale L., Roll S.C., *Impacts of Working From Home During COVID-19 Pandemic on Physical and Mental Well-Being of Office Workstation Users*

[49] A. Basilescu *apud* I.T. Ştefănescu, *Tratat teoretic şi practic de drept al muncii*, Universul Juridic, Bucureşti, 2014, p. 13.

DREPTUL PUBLIC ÎN ERA DIGITALĂ

PUBLIC LAW IN THE DIGITAL ERA

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII SUPLIMENT 2, ŞTIINȚE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-17

Falsul informatic. Interferenţe şi conexiuni cu alte infracţiuni

Computer Related Forgery. Interference and Connections With Other Crimes

Ruxandra Răducanu[1]

Rezumat: Infracţiunea de fals informatic reprezintă o incriminare nouă care conţine elemente ce se regăsesc şi în conţinutul altor infracţiuni, motiv pentru care, în practica judiciară s-a pus problema delimitării corecte a acestei infracţiuni de celelalte asemănătoare. Datele necorespunzătoare adevărului care rezultă în urma acţiunii tipice pot conduce la ideea inducerii în eroare, scopul de a produce consecinţe juridice poate echivala cu scopul de a obţine un folos patrimonial etc. Acest articol îşi propune să stabilească criterii clare care să evidenţieze particularitatea acestei incriminări, să o delimiteze, fără echivoc, de altele asemănătoare, luând în calcul obiectul juridic al acesteia şi specificitatea elementului său material.

Cuvinte-cheie: fals informatic; fraudă; pagubă; date informatice; acces ilegal la un sistem informatic

Abstract: The crime of tampering with computer data is an incrimination that contains elements that are also found in the content of other crimes, which is why, in judicial practice, the issue of the correct delimitation of this crime from other similar ones has been raised. Data that do not correspond to the truth resulting from the typical action may lead to the idea of misrepresentation, the purpose of producing legal consequences may be equivalent to the purpose of obtaining a patrimonial benefit. This study aims to establish clear criteria that highlight the particularity of this incrimination, to delimit it, unequivocally, from similar ones, taking into account its legal object and the specificity of its material element.

Keywords: tampering with computer data; fraud; damage; computer data; illegal access to a computer system

Infracţiunea de fals informatic completează capitolul falsurilor în înscrisuri, oferindu-se astfel protecţie şi acelor relaţii sociale care privesc încrederea publică în autenticitatea şi veridicitatea datelor informatice. Intenţia legiuitorului a fost de a acoperi toate faţetele prin care pot fi contrafăcute, falsificate înscrisurile, datele

[1] Profesor univ. dr., Facultatea de Drept, Universitatea din Craiova, e-mail: ruxandra.raducanu@edu.ucv.ro.

informatice fiind considerate drept „înscrisuri electronice”[2]. Apare, aşadar, firească opţiunea legiuitorului de a prelua această incriminare din legea specială, aşezarea ei în completarea falsurilor în înscrisuri, făcând vizibil cu uşurinţă obiectul juridic al acesteia.

În dorinţa sistematizării legii penale, Codul penal din 2009 a preluat mai multe incriminări din legi speciale. Un exemplu în acest sens este infracţiunea de fals informatic reglementată de dispoziţiile art. 325 C.pen. potrivit cărora *„Fapta de a introduce, modifica sau şterge, fără drept, date informatice ori de a restricţiona, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice, constituie infracţiune şi se pedepseşte cu închisoarea de la unu la 5 ani”.* Reglementarea iniţială se regăsea în Legea nr. 161/2003, Titlul III, art. 48, iar în actuala reglementare singura modificare priveşte limitele pedepsei, care au fost reduse.

Pentru comiterea infracţiunii de fals informatic este necesar să existe un sistem informatic funcţional, neputându-se lua în discuţie existenţa acestei infracţiuni în cazul inexistenţei unui sistem informatic în funcţiune[3]. Această cerinţă preexistentă poate, în aparenţă, să pună în discuţie opţiunea legiuitorului de reglementare a acestei infracţiuni în cadrul Titlului VI – Infracţiuni de fals, capitolul III – Falsuri în înscrisuri, de vreme ce în Titlul II – Infracţiuni contra patrimoniului, se regăseşte un capitol distinct, capitolul IV, destinat fraudelor comise prin sisteme informatice şi mijloace de plată electronice. Obiectul juridic al infracţiunii de fals informatic, rezultatul acesteia care se grefează pe încrederea publică în veridicitatea datelor informatice sunt argumente care justifică necesitatea încadrării acestei infracţiuni drept o infracţiune de fals. De altfel, datele necorespunzătoare adevărului trebuie să se subsumeze scopului de a putea fi folosite în vederea producerii unei consecinţe juridice, scop întâlnit şi în materia infracţiunii de fals material în înscrisuri oficiale.

Cu toate acestea, situaţia premisă a infracţiunii poate conduce la dificultăţi de încadrare şi la nevoia creării unor criterii clare de diferenţiere între infracţiunea de fals informatic de cea de fraudă informatică sau de alte infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice. Unele din cerinţele esenţiale pentru existenţa infracţiunii de fals informatic, cum ar fi săvârşirea faptei fără drept, datele necorespunzătoare adevărului care sunt rezultate din oricare din acţiunile incriminate, fac o diferenţă clară faţă de alte infracţiuni.

Astfel, delimitarea clară de alte incriminări asemănătoare trebuie să aibă în vedere prezenţa şi analiza unor cerinţe specifice infracţiunii de fals informatic.

Cele mai multe discuţii privesc raportul dintre infracţiunea de fals informatic şi cea de fraudă informatică, putând exista confuzie între cele două incriminări sau,

[2] C. Rotaru, A.-R. Trandafir, V. Cioclei, *Drept penal. Partea specială II*, Editura C.H. Beck, București, 2016, p. 386.

[3] G. Antoniu, T. Toader, V. Brutaru, Șt. Daneș, C. Duvac, I. Griga, I. Ifrim, Gh. Ivan, G. Paraschiv, I. Pascu, I. Rusu, M. Safta, I. Tanasescu, I. Vasiu, *Explicațiile noului Cod penal*, vol. IV, Editura Universul Juridic, București, 2016, p. 548.

dimpotrivă, concurs, fiind reţinută şi soluţia absorbiei falsului informatic în infracţiunea de fraudă informatică.

În aceste condiţii, dacă ne referim la infracţiunea de fraudă informatică, potrivit dispoziţiilor art. 249 C.pen., aceasta constă în *„introducerea, transmiterea, modificarea sau ştergerea de date informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane".*

Apreciem că cel mai important element care nu trebuie uitat şi nici neglijat priveşte stabilirea clară a **valorii sociale protejate** în cazul celor două infracţiuni. Frauda informatică reprezintă o infracţiune îndreptată împotriva patrimoniului, prin care se doreşte protejarea „integrităţii datelor informatice, securităţii sistemelor informatice şi patrimoniului unei persoane"[4]. De altfel, securitatea sistemelor informatice este inclusă în obiectul juridic al infracţiunii şi în opinia altor specialişti[5]. Spre deosebire, infracţiunea de fals informatic urmăreşte să protejeze încrederea publică în autenticitatea datelor informatice stocate într-un sistem informatic.

Este adevărat că modalităţile în care se poate comite elementul material al falsului intelectual se regăsesc şi în elementul material al infracţiunii de fraudă informatică, însă această împrejurare nu anulează valorile sociale diferite care sunt protejate prin cele două norme, care sunt evidenţiate şi de reglementarea lor în alte grupe de infracţiuni şi care impun soluţia concursului de infracţiuni pentru a asigura protejarea completă a valorilor sociale încălcate prin săvârşirea faptei.

De aceea, în doctrină[6] s-a apreciat că şi în situaţia în care sunt prezente elemente comune celor 2 infracţiuni (o modalitate comună a elementului material, producerea unei pagube, date necorespunzătoare adevărului, scopul obţinerii unui beneficiu), se menţine soluţia concursului de infracţiuni, deoarece una este o infracţiune contra patrimoniului, iar cealaltă o infracţiune de fals.

Producerea pagubei, ca rezultat evident şi anume precizat în textul normei de incriminare a fraudei informatice este o diferenţă faţă de infracţiunea de fals informatic şi motivul pentru care, în practica instanţelor, de cele mai multe ori, cele două infracţiuni sunt reţinute în concurs. Astfel, s-a retinut[7] concurs de infracţiuni în cazul „introducerii fără drept de date informatice şi a ataşării unei fotocopii a cărţii de identitate aparţinând altei persoane, precum şi a unui extras de cont modificat, pe numele acesteia pe platformele online ale unor instituţii financiare nebancare, rezultând date necorespunzătoare adevărului, respectiv atribuirea în fals a identităţii martorului, în scopul de a obţine un beneficiu material, respectiv contractarea unor împrumuturi în mod fraudulos, fiind cauzate pagube instituţiilor

[4] A. Boroi, *Drept penal. Parte specială,* Ed. 4, Editura C.H. Beck, Bucureşti, 2019, p. 291.

[5] T. Toader, *Drept penal român. Partea specială*, vol. I, Editura Universul Juridic, Bucureşti, 2019, p. 331.

[6] C. Rotaru, A.-R. Trandafir, V. Cioclei, *op. cit.,* p. 389.

[7] Judecătoria Ploieşti, sentinţa penală 1117/2021, [Online] la www.sintact.ro, accesat 08.12.2021.

financiare nebancare". S-a reţinut[8], de asemenea, concursul între cele 2 infracţiuni în cazul în care, în baza aceleiaşi rezoluţii infracţionale, s-a realizat introducerea fără drept de CNP-uri fictive aparţinând unor persoane inexistente şi modificarea, fără drept, a bazei de date a Agenţiei Judeţene pentru Plăţi şi Inspecţie Socială Maramureş, rezultând date necorespunzătoare adevărului şi, prin utilizarea aceluiaşi sistem informatic, au fost desfăşurate „activităţi ilicite specifice infracţiunii de fraudă informatică, constând în acte materiale distincte de a introduce şi modifica date informatice referitoare la programul privind alocaţia de stat pentru copii şi cel de indemnizaţie pentru creşterea copilului minor, cu scopul de a obţine un beneficiu material".

În practică sunt prezente şi soluţii argumentate în sensul absorbţiei infracţiunii de fals informatic în infracţiunea de fraudă informatică cu argumentarea că infracţiunea de „fals informatic este natural absorbită de infracţiunea de fraudă informatică, având în vedere că, în speţă, scopul activităţii infracţionale desfăşurate de inculpaţi a fost obţinerea unui beneficiu material. Pentru existenţa infracţiunii de fals informatic ar fi fost necesar ca fapta de a introduce, modifica, şterge date informatice să fie comisă cu scopul ca aceste modificări, în sens larg, să fie producătoare de consecinţe juridice, fără însă a se urmări în mod direct obţinerea unui beneficiu material"[9]. Soluţia se regăseşte şi în doctrină[10], care apreciază că frauda informatică este o infracţiune complexă ce absoarbe în conţinutul său infracţiunea de fals informatic.

Considerăm că, desi elementul material al infracţiunii de fals informatic se regăseşte, parţial, în elementul material al infracţiunii de fraudă informatică şi se poate reţine şi prezenţa celorlate cerinţe necesare existenţei falsului informatic, absorbţia acestei infracţiuni în infracţiunea de fraudă informatică nu poate fi admisă. În obiectul juridic al infracţiunii de fraudă informatică nu este inclusă protejarea încrederii publice – valoare socială ocrotită în cazul falsului –, iar soluţia absorbţiei ar lipsi de sancţiune atingerea adusă acestei valori.

Dacă analizăm comparativ cele două reglementări, se poate observa că elementul material al infracţiunii de fraudă informatică presupune şi împiedicarea în orice mod a funcţionării unui sistem informatic, ceea ce subliniază încă o data că acţiunea făptuitorului vizează, în principal, funcţionarea sistemului informatic, iar acţiunile care privesc datele informatice (introducerea, transmiterea, modificarea sau ştergerea de date informatice, restricţionarea accesului la aceste date) nu sunt comise **fără drept**, cerinţă precizată expres pentru existenţa falsului informatic. Cerinţa producerii unei pagube nu este de natura infracţiunii de fals

[8] Tribunalul Maramureş, sentinţa 12/2015, [Online] la www.legeaz.net, accesat 08.12.2021.

[9] Curtea de Apel Bucureşti, secţia a-II-a penală, decizia 1472 din 25 octombrie 2017, [Online] la www.rolii.ro, accesat 08.12.2021.

[10] N. Neagu, *Fraude comise prin sisteme informatice şi mijloace de plată electronice – variante speciale ale infracţiunii de înşelăciune?,* Revista Română de Drept penal al afacerilor nr. 3/2019; V. Dobrinoiu, N. Neagu, *Drept penal. Partea specială,* Editura Universul Juridic, Bucureşti, 2012, p. 272.

informatic, însă cerinţa realizării fără drept a oricăreia din acţiunile incriminate este esenţială pentru existenţa faptei.

Însăşi urmarea imediată a infracţiunii de fals informatic – **datele necorespunzătoare adevărului** – evidenţiază obiectul juridic al acesteia, necesitatea protejării încrederii publice.

De altfel, cele două elemente – săvârşirea fără drept a acţiunii incriminate şi datele necorespunzătoare adevărului rezultate – sunt, în mod constant evidenţiate în practică şi apreciate ca fiind definitorii pentru existenţa infracţiunii de fals informatic. În cazul în care crearea unei pagini de facebook în a cărei titulatură se foloseşte sigla unei societăţi completată cu o sintagmă cu conotaţie negativă, cu scopul de a atenţiona pe ceilalţi în privinţa serviciilor neserioase oferite de firmă, s-a apreciat că fapta nu este de natură a induce în eroare opinia publică, nu se realizează fără drept, deoarece inculpatul nu şi-a însuşit paternitatea siglei şi nici nu are ca urmare date necorespunzătoare adevărului, de vreme ce comentariile negative ale inculpatului erau urmarea neîndeplinirii obligaţiilor contractuale de către firmă[11]. Lipsa acestor elemente din conţinutul faptei conduce la concluzia neprevederii faptei în legea penală şi la soluţia achitării inculpatului.

Trebuie reţinut şi aspectul că ori de câte ori producerea pagubei este urmarea unei acţiuni de inducere în eroare care nu are legătură cu datele informatice, soluţia concursului de infracţiuni între înşelăciune şi fals informatic se reţine. În practică s-a reţinut[12] că în cazul postării unor anunţuri fictive pe diferite site-uri de internet în numele unor societăţi comerciale ce ofereau locuri de muncă în străinătate, anunţuri urmate de încheierea unor contracte de muncă false şi obţinerea unor comisioane drept compensaţie pentru prelucrarea dosarului de angajare, soluţia priveşte reţinerea concursului între înşelăciune şi fals informatic; s-a reţinut, de asemenea, aceeaşi soluţie, în cazul inducerii în eroare a părţii vătămate prin postarea pe reţeaua de internet a unui anunţ privind vânzarea unui tractor pe care inculpatul nu îl deţinea, având ca scop obţinerea de foloase materiale în mod fraudulos şi prejudicierea părţii vătămate ca urmare imediată. Având în vedere că frauda informatică fost privită ca o formă particulară de înşelăciune[13], ca o variantă specială a infracţiunii de înşelăciune[14], soluţia concursului falsului informatic cu infracţiunea de înşelăciune trebuie menţinută şi în cazul în care paguba este urmarea unui alt tip de înşelăciune – frauda informatică.

Şi în privinţa delimitării de infracţiunea de acces ilegal la un sistem informatic se poate pune problema confuziei între cele 2 infracţiuni, dar în structura infracţiunii de fals informatic nu este prevăzută condiţia accesării ilegale

[11] Curtea de Apel București, decizia nr. 1044/2017, [Online] la www.sintact.ro, accesat 08.12.2021.

[12] Curtea de Apel Timișoara, secția penală, decizia nr. 744/A/2016, [Online] la www.rolii.ro, accesat 08.12.2021; Tribunalul Olt, sentința penală nr. 284/2015, [Online] la www.sintact.ro, accesat 08.12.2021.

[13] Curtea de Apel Alba Iulia, s. pen., dec. nr. 821 din 10 octombrie 2017, [Online] la www.rolii.ro, accesat 08.12.2021.

[14] N. Neagu, *op. cit.*

a sistemului informatic pentru a introduce, modifica sau şterge, fără drept, date informatice sau pentru a restricţiona, fără drept, accesul la aceste date, ceea ce înseamnă că există posibilitatea comiterii falsului de o persoană autorizată să acceseze sistemul. Recent, Înalta Curte de Casaţie şi Justiţie s-a pronunţat[15] subliniind că noţiunea „fără drept" se raportează la datele informatice şi, prin urmare, la persoana care are dreptul de dispoziţie asupra acestor date, ceea ce face o diferenţă evidentă de infracţiunea de acces ilegal la un sistem informatic pentru care accesul este neautorizat. Mai mult, în cazul infracţiunii de fals informatic, nu are loc o intervenţie asupra unui sistem infomatic, ci acţiunea făptuitorului vizează şi se răsfrânge asupra datelor informatice, de aceea nu se poate vorbi de absorbţia infracţiunii de acces ilegal la un sistem informatic în falsul informatic, ci de concursul între cele 2 infracţiuni[16].

Considerăm că şi în această privinţă, soluţia concursului de infracţiuni poate fi fundamentată pe diferenţa obiectului juridic al fiecărei incriminări din concurs, prin accesul ilegal la un sistem informatic urmărindu-se „ocrotirea domiciliului informatic"[17], în timp ce la infracţiunea de fals informatic este evidentă nesocotirea încrederii publice în autenticitatea datelor informatice.

Discuţii pot să apară şi în legătură cu infracţiunea de alterare a integrităţii datelor informatice, reglementată de dispoziţiile art. 362 C.pen şi care constă în *„fapta de a modifica, şterge sau deteriora date informatice ori de a restricţiona accesul la aceste date, fără drept"*. Pe lângă faptul că modificarea, ştergerea datelor informatice sau restricţionarea accesului la acestea sunt întâlnite şi în elementul material al infracţiunii de fals informatic, toate aceste acţiuni tipice infracţiunii prevăzute de art. 362 sunt realizate fără drept, cerinţă întâlnită şi în elementul material al infracţiunii de fals informatic. Protecţia integrităţii datelor informatice se realizează prin incriminarea faptei de alterare a integrităţii datelor informatice, iar în situaţia în care acţiunile sunt săvârşite în scopul de a fi utilizate în vederea producerii unei consecinţe juridice, infracţiunea prevăzută de art. 362 C.pen. este absorbită în falsul informatic[18], reţinându-se doar această din urmă infracţiune. În cazul în care făptuitorul nu şi-a propus să utilizeze datele necorespunzătoare adevărului în vederea producerii unei consecinţe juridice, lipsind scopul

[15] Înalta Curte de Casație și Justiție, RIL nr. 4/2021, publicat în Monitorul Oficial nr. 171 din 19 februarie 2021, „Fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului, folosind ca nume de utilizator numele unei alte persoane și introducând date personale reale care permit identificarea acesteia, întrunește două dintre cerințele esențiale ale infracțiunii de fals informatic prevăzute în art. 325 din Codul penal, respectiv cea ca acțiunea de introducere a datelor informatice să fie realizată fără drept și cea ca acțiunea de introducere a datelor informatice să aibă ca rezultat date necorespunzătoare adevărului".

[16] Curtea de Apel Craiova, decizia nr. 827/2021, [Online] la www.sintact.ro, accesat 08.12.2021.

[17] I. Vasiu, L. Vasiu, *Informatică juridică şi drept informatic*, Editura Albastra, Cluj, 2002, p. 166.

[18] G. Antoniu, T. Toader ș.a, *op. cit.*, p. 552.

caracteristic falsului informatic, se va reţine infracţiunea de alterare a integrităţii datelor informatice.

În concluzie, infracţiunea de fals informatic reprezintă o incriminare distinctă, cu elemente particulare ce o diferenţiează de alte incriminări asemănătoare, ce presupune protecţia unei valori sociale bine evidenţiată, iar soluţia reţinerii în concurs cu infracţiunile menţionate anterior este justificată de argumente atât doctrinare, cât şi practice.

Referinţe

Antoniu G., Toader T., Brutaru V., Daneş Şt., Duvac C., Griga I., Ifrim I., Ivan Gh., Paraschiv G., Pascu I., Rusu I., Safta M., Tanasescu I., Vasiu I., *Explicaţiile noului Cod penal,* vol. IV, Editura Universul Juridic, Bucureşti, 2016

Boroi A., *Drept penal. Parte specială,* Ed. 4, Editura C.H. Beck, Bucureşti, 2019

Dobrinoiu V., Neagu N., *Drept penal. Partea specială,* Editura Universul Juridic, Bucureşti, 2012

Neagu N., *Fraude comise prin sisteme informatice şi mijloace de plată electronice – variante speciale ale infracţiunii de înşelăciune?,* Revista Română de Drept penal al afacerilor nr. 3/2019

Rotaru C., Trandafir A.-R., Cioclei V., *Drept penal. Partea specială II,* Editura C.H. Beck, Bucureşti, 2016

Toader T., *Drept penal român. Partea specială*, vol. I, Editura Universul Juridic, Bucureşti, 2019

Vasiu I., Vasiu L., *Informatică juridică şi drept informatic,* Editura Albastra, Cluj, 2002

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-18

Arma secretă a concurenţilor: cuvintele cheie pentru SEO

The Secret Weapon of the Competitors: the Keywords for SEO

Lucia Irinescu[1]

Rezumat: Motor de căutare, SEO şi cuvinte cheie: aceştia sunt termeni care contribuie direct la succesul unei afaceri pe internet. Identificarea uşoară online şi captarea traficului utilizatorilor de Internet sunt probleme cheie pentru toate companiile cu prezenţă digitală. Prin urmare, optimizarea vizibilităţii sale în paginile de căutare necesită optimizarea motoarelor de căutare (optimizarea motoarelor de *căutare* sau SEO), dar şi crearea strategiilor de achiziţie a traficului cu cuvinte cheie. Gigantul american Google, care deţine supremaţia în materia motoarelor de căutare, este totodată, şi campion al amenzilor încasate pentru acte de concurenţă neloială pe platformele digitale.

Cuvinte-cheie: piaţă digitală; concurenţă neloială; abuz de poziţie dominantă; Google

Abstract: Search engine, SEO and keywords: these are terms that directly contribute to the success of an internet business. Easy online identification and capturing Internet user traffic are key issues for all companies with a digital presence. Therefore, optimizing its visibility in search pages requires search engine optimization (search engine optimization or SEO), but also the creation of strategies to acquire keyword traffic. The American giant Google, which holds the supremacy in the field of search engines, is also the champion of the fines collected for acts of unfair competition on digital platforms.

Keywords: digital market; unfair competition; abuse of a dominant position; Google

1. Inteligenţa competitivă

Search Engine Optimization (SEO), în traducere *optimizare pentru motoare de căutare,* reprezintă un „proces de creştere (favorizare) a vizibilităţii site-urilor web sau a paginilor web în rezultatele căutării unui motor de căutare, iar acesta din urmă, la rândul lui, utilizează un algoritm precis prin care „alege” ordinea paginilor pentru anumite căutări, în funcţie de relevanţa paginilor respective”[2].

Deşi denumirea pare una destul de sofisticată şi mecanismul unul complicat, noţiunea de SEO a apărut în anii ‘90, odată cu apariţia motoarele de căutare care indexau conţinutul de pe web şi reprezentau, totodată, o sursă importantă de trafic pentru web. De fapt, acesta este şi momentul în care specialiştii din această

[1] Conferenţiar univ. dr., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iaşi, e-mail: lirinescu@yahoo.com.

[2] [Online] la https://ro.wikipedia.org/wiki/Optimizare_pentru_motoare_de_c%C4%83utare, accesat 29.11.2021.

industrie au realizat faptul că pot controla procesul de creştere a vizibilităţii paginilor web. Astăzi, conform statisticilor, există peste 6 miliarde de site-uri web la nivel global, peste 4 miliarde de oameni folosesc zilnic internetul, cautând informatii pe web sau accesează reţelele sociale, peste 70 de mii de site-uri sunt piratate, iar Google contabilizează aproximativ 2,5 trilioane de căutări pe an[3].

În condiţiile evoluţiei tot mai rapide a tehnologiilor digitale, pe care, în prezent, se bazează toate sectoarele economiei, creşterea competitivităţii pe piaţa digitală reprezintă o provocare atât pentru actorii de pe piaţă, cât şi pentru autorităţile de concurenţă. Dezvoltarea mediului online şi accesibilitatea la internet a populaţiei au condus la extinderea acestor mecanisme pe toate palierele existenţei noastre, acoperind o gamă largă de activităţi, comerciale şi necomerciale precum: reţele sociale, sisteme de plată, comparatoare de preţuri, comerţ online, mass-media, platforme de aplicaţii, motoare de căutare etc.

Mediul de afaceri a recurs la implementarea acestor tehnologii în activitatea lor, din dorinţa de a creşte numărul de clienţi, de a se extinde peste graniţele fizice, de a optimiza procesele operaţionale, de a reducere costurile, de a monitoriza pieţele şi concurenţii etc. Platformele online au condus la apariţia unor noi modele de afaceri, bazate pe noile tehnologii şi pe accesul la piaţa globală, au unit, virtual, vânzătorii, cumpărătorii şi intermediarii şi au sporit şi posibilităţile de alegere ale consumatorilor.

Din punct de vedere al concurenţei, aceste tehnologii pot conduce la schimbarea dinamicii pieţei, oferind astfel jucătorilor deja prezenţi pe piaţă un avantaj competitiv concomitent cu o creştere a riscului de apariţie a unor posibile abuzuri de poziţie dominantă. Potenţialul comercial uriaş al internetului permite, din păcate, şi apariţia aşa-zişilor *spammers*, care încearcă să manipuleze ilegal vizibilitatea site-urilor, profitând de criteriile de ordonare (*ranking*), adică de acei factori care duc la o poziţionarea mai bună în paginile cu rezultate. Din această perspectivă, identificăm două tipuri de SEO:

- optimizare internă (*on-site optimization*), atunci când măsurile de optimizare pot fi influenţate numai de echipa SEO;

- optimizare externă (*off-site optimization*), atunci când măsurile de optimizare nu mai depind de echipa SEO, ci de o serie de indicatori de calitate, performanţă, popularitate.

Din punct de vedere al gradului de moralitate al tehnicilor utilizate, SEO poate fi împărţit în:

- *white hat SEO*, atunci când promovarea corespunde întocmai politicilor sugerate de către motoarele de căutare;

- *black hat SEO*, dacă scopul promovării este de a manipula percepţia motoarelor de căutare cu privire la relevenţa şi importanţa site-ului, cum ar fi, de exemplu: folosirea excesivă a cuvintelor cheie în titluri şi conţinutul paginilor, ascunderea cuvintelor în spatele imaginilor etc;

[3] A se vedea [Online] la www.datahost.ro, accesat 29.11.2021.

- *grey hat SEO*, o combinaţie între primele două forme, în care deşi se respectă unele criterii morale, anumite practici sunt sancţionabile.

Prin urmare, scopul SEO este acela de a creşte traficul, baza de clienţi, profitul şi, chiar şi atunci când eşti pe primul loc pe un motor de căutare important, precum Google, Yahoo!, Bing, cuvintele cheie pot fi folosite pentru extinderea pe alte pieţe.

Analiza SEO a concurenţei reprezintă descoperirea motivelor pentru care un anumit site are o poziţionare bună pe un motor de căutare în baza unor cuvinte cheie. De regulă, motoarele de căutare analizează comportamentul oamenilor, preferinţele acestora, de ce tip de conţinut sunt atraşi şi dă prioritate conţinutului pe care utilizatorul îl îndrăgeşte, în funcţie de cât timp petrece acesta pe o pagină, în timp ce algoritmii din spatele motoarelor se schimbă în permanenţ şi se adaptează în funcţie de comportamentul consumatorului. Mai mult, Google, de exemplu, vrea ca utilizatorii să folosească foarte mult motoarele de căutare. Privind mai atent concurenţii prin prisma SEO, pot fi identificate cuvintele cheie şi expresiile extrem de relevante mulţumită cărora aceştia se clasează pe primele locuri în rezultatele căutării, care par a fi cele mai mari atuuri şi puncte slabe ale acestora ca afacere, de ce au succes sau eşuează campaniile de promovare ale acestora etc.

2. Marketingul în mediul online şi Google Ads

2.1. Marketingul în mediul online

Marketingul performant se realizează prin înţelegerea instrumentelor şi a mediului în care sunt utilizate. Astăzi, marea majoritate a întreprinderilor au înţeles că prezenţa în mediul *on-line* cu o pagină web este un *must* pentru buna funcţionare a afacerii. Instrumentele utilizate în acest sens sunt numeroase: SEO, *Google Adwords*, *newsletter marketing*, *blog marketing* etc.[4]

Marketingul pe bază de SEO constă în poziţionarea de către motoarele de căutare a unui *website* în paginile sale. Pentru a fi luat în considerare de către algoritmii motoarelor de căutare, *website*-ul va trebui să aibă un design curat, aerisit si modern, un *branding* dedicat şi de regulă foarte mult text. Avansarea în poziţiile unui motor de căutare va cântări mult la imaginea, prestigiul şistabilitatea în piaţă a afacerii şi va aduce companiei sau magazinului online propriu mai mulţi clienţi, în mod constant, fără investiţii masive în publicitate.

Promovarea prin marketing online plătit presupune o publicitate plătită prin diverse forme: plata *per click*, publicitatea prin *banner* etc. care va poziţiona la vedere produsul sau serviciul doar pe perioada cât va exista un buget alocat campaniei publicitare. Când acest buget este epuizat, reclama va dispărea în favoarea altor companii concurente, al căror buget încă nu s-a terminat. Marea majoritate a companiile apelează la un mix publicitar între marketing online şi SEO.

[4] Pentru detalii, a se vedea E. Mitan, *Sisteme inteligente de marketing*, în Revista Română de Informatică şi Automatică, vol. 21, nr. 1/2011, [Online] la https://rria.ici.ro/wp-content/uploads/2011/03/05-art.-Electra-Mitan.pdf, accesat 29.11.2021.

Promovarea produsului în mod agresiv este o practică online folosită în scopul de a utiliza toate elementele de marketing web şi a produce o reacţie rapidă din partea publicului ce navighează în mediul online. În acelaşi timp, tehnica de promovare agresivă include însă ambele variante, respectiv marketing online si SEO.

Publicitatea şi concurenţa sunt strâns legate între ele, deoarece publicitatea stimulează concurenţa; legea practicilor anticoncurenţiale se poate ocupa şi de conţinutul mesajului publicitar, dar mai ales controlează contractele şi condiţiile de acces la publicitate.

Motorul de căutare Google deţine, în prezent, o cotă de piaţă de 92,46%, începând cu anul 2019, lăudându-se cu cel mai popular browser din lume, Chrome, precum şi cu sistemul de operare Android. De asemenea, controlează Gmail, cel mai mare serviciu de e-mail din lume, precum şi Youtube, al doilea cel mai mare motor de căutare din lume. Acest proces permite ca utilizatorii să se afle întotdeauna în ecosistemul Google şi să se întoarcă înapoi la motorul de căutare principal, asigurându-i o poziţie dominantă.

Google Ads reprezintă un instrument de marketing oferit de Google companiilor. Principiul de funcţionare *Google Ads* presupune crearea unui anunţ de tipul text, imagine, *gif*, *html*, care să conţină cuvinte cheie legate de produsele sau serviciile companii respective; atunci când utilizatorii vor introduce pe motorul de căutare Google cuvintele cheie respective, vor fi direcţionaţi spre site-ul companiei care a publicat anunţul. În plus, sistemul permite ajustarea bugetului, a publicului ţintă, în funcţie de vârstă, arie geografică, studii etc., pentru a ţinti cât mai exact potenţialii clienţi sau întreruperea anunţului în orice moment. Aşadar, *AdSense for Search* funcţionează ca o platformă de intermediere a publicităţii asociate cu căutările online.

2.2. Decizii de sancţionare a gigantului Google pentru abuzul de poziţie dominantă pe piaţa publicităţii on-line

La o primă vedere, deşi *Google Ads* pare să aducă numai beneficii companiilor care utilizează acest serviciu, autorităţile de concurenţă din statele membre, dar şi Comisia Europeană au analizat modul de funcţionare al acestei publicităţi personalizate asociată căutărilor şi au ajuns la concluzia că practicile Google au împiedicat concurenţa pe această piaţă.

La 20 martie 2019, Comisia Europeană a amendat Google cu 1,49 EUR miliarde de euro[5] deoarece a constatat că Google a inclus în contractele sale clauze de exclusivitate prin care interzicea editorilor să plaseze pe paginile lor de rezultate ale căutării orice anunţuri publicitare asociate cu căutările online aparţinând concurenţilor Google. Ulterior**,** Google a început treptat să înlocuiască clauzele de exclusivitate cu aşa-numitele clauze de „plasamente premium" (*Premium Placement*) prin care impunea editorilor să rezerve pentru anunţurile publicitare ale Google cel mai profitabil spaţiu de pe paginile lor cu rezultate ale căutărilor şi

[5] Decizia Comisiei din 20 martie 2019 în cazul AT.40411 Google Search (AdSense), [Online] la https://ec.europa.eu/competition/antitrust/cases/dec_docs/40411/40411_1619_11.pdf, accesat 29.11.2021.

să includă pe site-urile lor un număr minim de anunţuri publicitare aparţinând Google. Drept rezultat, concurenţii Google au fost împiedicaţi să îşi plaseze anunţurile publicitare asociate cu căutările în spaţiile cele mai vizibile şi mai accesate ale paginilor de rezultate de căutare ale site-urilor. Google a inclus şi clauze care impuneau editorilor să solicite o aprobare scrisă din partea Google înainte de a modifica modul în care erau afişate anunţurile publicitare ale concurenţilor. Acest lucru a însemnat că Google putea controla cât de atrăgătoare şi, prin urmare, cât de accesate puteau fi anunţurile publicitare ale concurenţilor săi.

Comisia a ajuns la concluzia că, prin comportamentul său, Google a denaturat concurenţa, a adus prejudicii consumatorilor şi a sufocat inovarea. Concurenţii Google Microsoft şi Yahoo nu au putut să dezvolte şi să ofere servicii de intermediere a publicităţii asociate cu căutările online alternative celor oferite de Google. Drept rezultat, proprietarii site-urilor aveau opţiuni limitate de monetizare a spaţiului de pe aceste site-uri şi erau forţaţi să se bazeze aproape în exclusivitate pe Google[6].

În noiembrie 2019, Autoritatea de Concurenţă din Franţa a iniţiat o investigaţie împotriva gigantului american Google, pentru abuz de poziţie dominantă pe piaţa serviciilor de intermediere în materie de anunţuri publicitare asociate cu căutările online. Autoritatea de concurenţă a solicitat ca Google să clarifice regulile de utilizare a serviciului *Google Ads* şi a procedurilor prin care conturile utilizatorilor pot fi închise sau suspendate. Plângerea a fost formulată de către o companie franceză, Gibmedia, care a considerat că Google a tratat-o într-un mod abuziv, întrucât i-a închis contul şi nu i-a mai permis accesul la platforma sa de publicitate. Gibmédia activează în cadrul serviciului de informaţii cu plată şi este membră a Asociaţiei Franceze de Informaţii telefonice (AFRT) care reuneşte operatorii de servicii de informare telefonică cu plată.

Google a motivat închiderea contului de utilizator deoarece Gibmedia folosea reclame înşelătoare. În urma investigaţiei, la 19 decembrie 2019, Autoritatea de concurenţă franceză a decis aplicarea unei amenzi de 150 milioane de euro, obligând totodată Google să ofere mai multă transparenţă, claritate şi consistenţă

[6] Comisia Europeană a amendat Google LLC şi societatea-mamă Alphabet Inc. în repetate rânduri pentru încălcarea normelor antitrust ale UE. În iunie 2017, Comisia a amendat Google cu 2,42 miliarde EUR pentru că a abuzat de poziţia dominantă a motorului său de căutare, ceea ce a conferit un avantaj ilegal serviciului propriu al Google de comparare a preţurilor . Decizia Comisiei din 27 iunie 2017 în cazul AT. 39740- Google Search (Shopping), [Online] la https://eur-lex.europa.eu/legal- content/EN/TXT/?qid= 1516198535804&uri=CELEX:52018XC0112(01), accesat 29.11.2021. În iulie 2018, Comisia a amendat Google cu 4,34 miliarde EUR pentru practici ilegale legate de dispozitivele mobile care utilizează sistemul de operare Android pentru a consolida poziţia dominantă a motorului de căutare al Google. Decizia Comisiei din 18 iulie 2018 în cazul AT. 40099- Google Andoid, [Online] la https://ec.europa.eu/competition/antitrust/ cases/dec_docs/ 40099/40099_9993_3.pdf, accesat 29.11.2021. Pentru detalii, a se vedea L. Irinescu, *Noi provocări în era digitală. Politica de concurenţă*, în Analele UAIC, Tomul LXV, Supliment/2019, [Online] la http://pub.law.uaic.ro/files/articole/2019/vols/4.irinescu.pdf, accesat 29.11.2021.

cu privire la modul în care aplică regulile referitoare la reclamele care sunt afişate lângă rezultatele căutării, să clarifice textul Regulilor *Google Ads* care sunt menite să protejeze utilizatorii motorului său de căutare online *Google Search* împotriva reclamelor şi site-urilor rău intenţionate. Autoritatea de Concurenţă a considerat că comportamentul Google era de natură să caracterizeze o încetare bruscă a relaţiilor comerciale cu această societate în condiţii care nu erau obiective şi transparente şi puteau fi considerate discriminatorii în comparaţie cu alţi furnizori de servicii care plătesc informaţii telefonice în 118[7]. Totodată, Autoritatea de Concurenţă a constatat, în stadiul anchetei, o lipsă de transparenţă şi obiectivitate în aplicare şi în definirea regulilor *Google Ads* referitoare la „Vânzarea articolelor gratuite" şi regulile secţiunii „Declaraţii înşelătoare". În aceeaşi cauză, Curtea de Apel din Paris a reţinut, de asemenea, că prin luarea deciziei de modificare a regulilor *Google Ads* şi de excludere a serviciilor de informaţii telefonice din serviciul *Google Ads*, compania Google, care deţine o poziţie dominantă pe piaţa de publicitate online, încalcă în mod deliberat măsurile impuse acesteia în Franţa de către Autoritatea de Concurenţă şi constituie o încălcare vădită a obligaţiilor sale care justifică suspendarea aplicării acestei modificări[8].

Compania Google a ajuns de mai multe ori în faţa instanţelor din Paris. Într-o altă speţă[9], *Bureau Carte Grise* care desfăşoara, în numele clienţilor săi, proceduri necesare obţinerii certificatelor de înmatriculare a autovehiculelor, a achiziţionat, pentru promovarea activităţii sale, cuvinte cheie prin intermediul *Google Ads*, care permiteau afişarea anunţurilor sale pe paginile de rezultate ale motorului de căutare Google. Google a informat compania *Bureau Carte Grise* cu privire la modificarea condiţiilor generale ale serviciului său *AdWords* şi a interzis distribuirea de reclame pentru servicii referitoare la documente oficiale accesibile direct dintr-o administraţie publică. Această măsură a provocat un prejudiciu iminent companiei *Bureau Carte Grise* prin faptul că Google, profitând de poziţia sa dominantă pe piaţa de publicitate online, i-a interzis să practice comerţul electronic. Instanţele au menţinut amenda aplicată de către Autoritatea de concurenţă şi au dispus restabilirea publicării şi difuzării reclamelor şi cuvintelor cheie ale companiei *Bureau Carte Grise* în legătură cu serviciul de eliberare a certificatelor de înmatriculare şi a certificatelor de înmatriculare a vehiculelor.

În iunie 2021, Google a fost din nou amendat de către aceeaşi Autoritate de concurenţă din Franţa pentru abuz de poziţie dominantă pe piaţa de publicitate online[10]. Aceasta a fost prima decizie a unei autorităţi de concurenţă care s-a bazat pe o analiză complexă a procedeelor algoritmice pe care se bazează *businessul* de *advertising online.*

[7] Decizia nr. 19 -D-26 din 19 decembrie 2019 (decizia Amadeus). A se vedea şi Decizia din 31 ianuarie 2019 nr. 19-MC-01, Lexis 360 beta.

[8] Curtea de Apel din Paris, Hotărârea din 15 ianuarie 2021 - nr. 20/06303, Lexis 360 beta.

[9] Curtea de Apel din Paris, Hotărârea din 28 aprilie 2021- nr. 21/04568, Lexis 360 beta.

[10] Autoritatea de Concurenţă din Franţa, Hotărârea nr. 21-D-11 din 7 iunie 2021, publicată în Jurnalul Oficial nr. 122 din 26 mai 2019,Lexis 360 beta.

Investigaţia autorităţii franceze a fost declanşată de o plângere depusă de grupul de presă *News Corp*, cu sediul în SUA, ziarul francez *Le Figaro* şi grupul de presă belgian *Rossel* împotriva gigantului Google (sunt companii specializate în crearea, editarea şi distribuţia de conţinut pentru persoane fizice şi profesionişti, legate în principal de ştiri şi informaţii).

Pentru a comercializa spaţiile publicitare prezente în site-urile şi aplicaţiile lor, editorii folosesc diferite tipuri de tehnologii, în special tehnologii de ad server şi tehnologii de platformă pentru vânzarea spaţiilor publicitare: vânzarea directă şi vânzarea programatică. Vânzările directe se bazează pe un acord încheiat direct între editorul site-ului, sau al aplicaţiei mobile, şi agentul de publicitate, eventual reprezentat de o agenţie. Aceste acorduri se bazează în general pe obiective pe o perioadă de timp, fie ca număr de afişări, fie ca procent de afişări. Vânzarea directă se realizează pe serverul de anunţuri, care este un instrument de afişare a reclamelor pe site-ul sau aplicaţia mobilă a editorului. Platformele pentru vânzarea programatică a spaţiului publicitar sunt „pieţe" în care cumpărătorii de spaţiu publicitar se întâlnesc cu editorii care doresc să vândă spaţiu publicitar. Pentru a-şi putea optimiza veniturile şi a-şi maximiza şansele de a vinde un anumit spaţiu publicitar, editorii vând în general acelaşi spaţiu publicitar prin mai multe platforme de licitaţie simultan. În schimb, editorii folosesc în general un singur server de anunţuri pentru a organiza competiţia între diferite platforme de vânzare. Interoperabilitatea unui *ad server* cu platformele de vânzare determină aşadar atât veniturile pe care editorii le obţin din spaţiile lor publicitare, cât şi atractivitatea platformelor de licitaţie.

Platformele de vânzare a spaţiului publicitar (*Supply Side Platform* - SSP) sunt astăzi intermediarii preferaţi pentru cei mai importanţi editori. Pe lângă platformele *AdSense* şi *AdMob*, care oferă funcţionalităţi limitate de server de anunţuri pentru mediile de aplicaţii mobile, Google a dezvoltat o nouă tehnologie de publicitate online oferită editorilor ţi anume serverul de anunţuri *DoubleClick for Publishers* („DFP") şi platforma de spaţiu publicitar *DoubleClick Ad Exchange* („AdX"). În iunie 2018, Google a integrat DFP şi AdX sub denumirea *Google Ad Manager* („GAM"), care constituie oferta de server şi platformă destinată editorilor.

Autoritatea de concurenţă a observat că Google a implementat practici menite să se asigure că serverul său de publicitate DFP îşi promovează platforma de vânzare a spaţiului publicitar AdX, în detrimentul atât al furnizorilor concurenţi, cât şi al performanţei inventarelor de publicitate online ale editorilor. De asemenea, Google a implementat practici menite să se asigure că platforma sa AdX favorizează serverul său DFP. În primul rând, serverul publicitar DFP a favorizat platforma de vânzări AdX, în special indicându-i preţul oferit de platformele SSP concurente. AdX a folosit, de fapt, aceste informaţii pentru a optimiza procesul de licitaţie pe care l-a implementat, în special prin variarea comisionului primit la impresiile vândute în funcţie de intensitatea concurenţială. În al doilea rând, Google a impus limitări tehnice şi contractuale privind utilizarea platformei AdX prin intermediul unui server de anunţuri terţă parte. Prin urmare, condiţiile de interacţiune oferite

clienţilor serverelor de anunţuri terţe au fost inferioare condiţiilor de interacţiune dintre DFP şi AdX, care penalizau atât SSP-urile terţe, cât şi clienţii editorilor.

Practicile nu au afectat numai concurenţii Google. Editorii site-ului au fost, de fapt, lipsiţi şi de posibilitatea de a folosi pe deplin concurenţa dintre diferitele SSP. Drept urmare, au pierdut venituri care ar fi trebuit asociate cu vânzarea stocurilor lor la preţurile rezultate în urma licitaţiilor de alocare a acestora. În special, editorii nu au putut obţine preţuri de achiziţie mai mari de la SSP-uri şi, în special, de la platforma AdX Google. Clienţii finali afectaţi de aceste practici corespund în speţă tuturor editorilor de site-uri web şi aplicaţii mobile, şi în special grupurilor de presă[11].

Google a fost amendată cu 220 de milioane de euro şi s-a angajat să îmbunătăţească modul în care serviciile *Ad Manager* lucrează cu alte platforme, începând cu primul trimestru din 2022, pe o perioadă de 3 ani.

Recent, Google a mai făcut obiectul unor investigaţii ale autorităţilor de concurenţă din Italia[12] care l-a sancţionat pentru abuz de poziţie dominantă.

3. Spre o nouă piaţă digitală

Pe cale de consecinţă, recent, statele membre au căzut de acord asupra adoptării a două seturi de legi importante menite să reglementeze activitatea online a companiilor Amazon, Apple, Google şi Facebook. Autorităţile de concurenţă din statele membre salută iniţiativa Comisiei de a elabora un set de criterii obiective strict definite - *Actul legislativ privind pieţele digitale (APD)*[13]- pentru a califica o mare platformă online drept „controlor al fluxului de informaţie". Aceste criterii vor fi îndeplinite dacă o întreprindere are o poziţie economică puternică, un impact semnificativ asupra pieţei interne şi este activă în mai multe ţări din UE, are o poziţie de intermediere puternică, adică face legătura între un număr mare de utilizatori şi de întreprinderi şi deţine (sau este pe punctul de a avea) o poziţie solidă şi durabilă pe piaţă, ceea ce înseamnă că este stabilă în timp[14].

Propunerea este coerentă cu strategia digitală a Comisiei în ceea ce priveşte contribuţia sa la asigurarea unei economii digitale echitabile şi competitive, unul dintre cei trei piloni principali ai orientării politice şi ai obiectivelor anunţate în

[11] L. Arcelin, *„Fasc. 797: Publicité et concurrence"*, în JurisClasseur Concurrence – Consommation 30/10/2020, Legis 360 beta.

[12] Autoritatea de Concurență din Italia a impus o amendă de 20 de milioane de euro pentru Google și Apple, egal repartizată între cei doi giganți, pentru că au apelat la metode agresive de colectare a datelor utilizatorilor și de folosire a lor în scop comercial.

[13] A se vedea Propunere de Regulament privind piețe contestabile și echitabile în sectorul digital din 15 decembrie 2020, COM(2020) 842, [Online] la https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52020PC0842&from=ro, accesat 29.11.2021.

[14] Pentru detalii, a se vedea M. M. Vignal, D. Heintz, M. Lécole, *Droit de la concurrence - Comment appréhender les abus et l'utilisation des données dans la relation d'une plateforme avec ses partenaires contractuels?,* în Contrats Concurrence Consommation nr. 12/01.12.2020, Legis 360 beta.

comunicarea intitulată „Conturarea viitorului digital al Europei". Aceasta va constitui un cadru eficace şi proporţional pentru abordarea problemelor din economia digitală care, în prezent, nu pot fi soluţionate sau nu pot fi soluţionate în mod eficace.

Capitolul I stabileşte dispoziţiile generale, inclusiv obiectul, scopul şi domeniul de aplicare al regulamentului, inclusiv efectul său de armonizare în ceea ce priveşte anumite legislaţii naţionale (articolul 1), precum şi definiţiile termenilor utilizaţi în propunere şi obiectivele acesteia (articolul 2).

Capitolul II conţine dispoziţiile privind desemnarea *gatekeeperilor*. Mai precis, acesta stabileşte condiţiile în care furnizorii de servicii de platformă esenţiale ar trebui desemnaţi drept *gatekeeperi*, fie pe baza criteriilor cantitative (printr-o prezumţie care poate fi combătută prin probe contrarii), fie în urma unei evaluări de la caz la caz în cursul unei investigaţii de piaţă (articolul 3). În plus, se stabilesc, de asemenea, condiţiile în care desemnarea unui *gatekeeper* poate fi reexaminată şi obligaţia de a revizui periodic o astfel de desemnare (articolul 4).

Capitolul III stabileşte practicile *gatekeeperilor* care limitează contestabilitatea şi care sunt neloiale. În special, acesta stabileşte obligaţiile autoexecutabile (articolul 5) şi obligaţiile susceptibile să fie clarificate (articolul 6) pe care ar trebui să le respecte *gatekeeperii* desemnaţi în ceea ce priveşte fiecare dintre serviciile lor de platformă esenţiale enumerate în decizia de desemnare relevantă. În plus, se stabileşte un cadru pentru un posibil dialog între *gatekeeperul* desemnat şi Comisie în ceea ce priveşte măsurile pe care *gatekeeperul* le pune în aplicare sau intenţionează să le pună în aplicare în vederea respectării obligaţiilor prevăzute la articolul 6 (articolul 7). Regulamentul stabileşte, de asemenea, condiţiile în care obligaţiile pentru un anumit serviciu de platformă esenţial pot fi suspendate în circumstanţe excepţionale (articolul 8) sau poate fi acordată o derogare din motive de interes public (articolul 9). Dispoziţiile suplimentare din acest capitol stabilesc un mecanism de actualizare a listei de obligaţii (articolul 10); o clarificare a faptului că obligaţiile prevăzute în regulament se aplică indiferent dacă practica relevantă a *gatekeeperului* desemnat este de natură contractuală, comercială, tehnică sau de orice altă natură (articolul 11); obligaţia de a notifica orice concentrare preconizată în sensul Regulamentului UE privind concentrările economice (articolul 12) şi o obligaţie impusă *gatekeeperului* desemnat de a supune unui audit independent orice tehnici de stabilire a profilului consumatorilor pe care *gatekeeperul* le aplică serviciilor sale de platformă esenţiale (articolul 13).

Capitolul IV prevede norme pentru efectuarea investigaţiilor de piaţă, în special cerinţe de procedură pentru deschiderea unei investigaţii de piaţă (articolul 14) şi norme pentru efectuarea diferitelor tipuri de investigaţii de piaţă: (i) desemnarea unui *gatekeeper* (articolul 15), (ii) investigarea cazurilor de neconformitate sistematică (articolul 16) şi (iii) investigarea noilor servicii de platformă esenţiale şi a noilor practici (articolul 17).

Capitolul V conţine dispoziţiile privind punerea în aplicare şi asigurarea respectării prezentului regulament. Acesta prevede cerinţele de procedură pentru deschiderea procedurilor (articolul 18). De asemenea, capitolul stabileşte norme

referitoare la diferite instrumente care pot fi utilizate în contextul investigaţiilor de piaţă sau al procedurilor în temeiul regulamentului. Printre acestea se numără capacitatea Comisiei de a solicita informaţii (articolul 19), de a desfăşura interviuri şi de a lua declaraţii (articolul 20), de a efectua inspecţii la faţa locului (articolul 21), de a adopta măsuri provizorii (articolul 22) şi de a face măsurile voluntare obligatorii pentru *gatekeeperi* (articolul 23), precum şi de a monitoriza conformitatea acestora cu regulamentul (articolul 24). În caz de neconformitate, Comisia poate emite decizii de neconformitate (articolul 25) şi poate impune amenzi (articolul 26) şi penalităţi cu titlu cominatoriu (articolul 27) pentru încălcări ale regulamentului de către *gatekeeperi*, precum şi pentru furnizarea de informaţii incorecte, incomplete sau înşelătoare în contextul investigaţiei. Regulamentul stabileşte, de asemenea, un termen de prescripţie pentru impunerea de sancţiuni şi pentru executarea acestora (articolele 28 şi 29). Mai multe dispoziţii din acest capitol stabilesc garanţiile procedurale în faţa Comisiei, în special dreptul de a fi audiat şi dreptul de acces la dosar (articolul 30) şi protecţia secretului profesional (articolul 31). Acesta prevede, de asemenea, consultarea Comitetului consultativ pentru pieţele digitale instituit prin prezentul regulament înainte de a adopta deciziile individuale identificate adresate *gatekeeperilor* (articolul 32). În cele din urmă, regulamentul prevede posibilitatea ca trei sau mai multe state membre să solicite Comisiei deschiderea unei investigaţii de piaţă în temeiul articolului 15 (articolul 33).

Capitolul VI conţine dispoziţii generale suplimentare, cum ar fi obligaţia de a publica un set identificat de decizii individuale adoptate în temeiul regulamentului (articolul 34), o clarificare a faptului că Curtea de Justiţie a Uniunii Europene are competenţă nelimitată în ceea ce priveşte amenzile şi penalităţile cu titlu cominatoriu (articolul 35), precum şi posibilitatea de a adopta acte de punere în aplicare (articolul 36) şi acte delegate (articolul 37). În cele din urmă, celelalte dispoziţii din acest capitol includ clauza de revizuire (articolul 38) şi specificarea intrării în vigoare şi a datelor de aplicare a regulamentului (articolul 39).

Concluzii

Serviciile digitale în general şi platformele online în special joacă un rol din ce în ce mai important în economie, în special pe piaţa internă, oferind noi oportunităţi de afaceri în Uniune şi facilitând comerţul transfrontalier. serviciile de intermediere online, motoarele de căutare online, sistemele de operare, reţelele de socializare online, serviciile oferite de platformele de partajare a materialelor video, serviciile de comunicaţii interpersonale care nu se bazează pe numere, serviciile de *cloud computing* şi serviciile de publicitate online au capacitatea de a afecta un număr mare de utilizatori finali şi comerciali, ceea ce determină un risc de practici comerciale neloiale.

Referinţe

Arcelin L., *Fasc. 797: Publicité et concurrence,* în JurisClasseur Concurrence – Consommation 30/10/2020, Legis 360

Irinescu L., *Noi provocări în era digitală. Politica de concurenţă*, în Analele UAIC, Tomul LXV, Supliment/2019

Mitan E., *Sisteme inteligente de marketing*, în Revista Română de Informatică şi Automatică, vol. 21, nr. 1/2011

Vignal M. M., Heintz D., Lécole M., *Droit de la concurrence -Comment appréhender les abus et l'utilisation des données dans la relation d'une plateforme avec ses partenaires contractuels?,* în Contrats Concurrence Consommation nr. 12/01.12.2020, Legis 360 beta

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-19

Suveranitatea digitală – viitorul spaţiului virtual?

Is Cybersovereignty the Future of Cyberspace?

Carmen Moldovan[1]

Rezumat: Conceptul de suveranitate digitală a fost promovat intens de către China şi Federaţia Rusă şi se doreşte a fi o transpunere în mediul virtual a principiului suveranităţii din dreptul internaţional public. De esenţa sa este opoziţia faţă de ideea libertăţii internetului în lipsa reglementărilor din partea statelor. Prezenta lucrare îşi propune să exploreze, dintr-o perspectivă critică, principalele trăsături şi implicaţii ale suveranităţii digitale, prin trimitere la principiile dreptului internaţional. Până în prezent, la nivelul ONU s-a cristalizat concluzia aplicabilităţii principiilor dreptului internaţional în *Cyberspace* (inclusiv a principiului suveranităţii), însă nu este clar dacă aplicarea acestora se realizează în aceeaşi parametri şi având acelaşi sens ca în spaţiul fizic.

Cuvinte-cheie: principii; ONU; reglementare; suveranitate; aplicare teritorială

Abstract: Cybersovereignty is a concept highly supported by China and the Russian Federation, considering it as an application of the principle of state sovereignty. In essence, it is opposed to the idea of an open Internet outside State regulations. The aim of this paper is to critically explore the main features and implications of the concept of Cybersovereignty by reference to the basic principle of sovereignty in International Law. At this date, within the United Nations the conclusion of specialized working groups is that principles and norms of International Law are applicable in Cyberspace. However, it is far from clear if the same parameters and meaning as in the physical space are applicable.

Keywords: principles; UN; regulation; sovereignty; territorial application

Introducere

Dezvoltarea internetului a avut un efect omniprezent asupra comunicaţiilor şi tehnologiei, afectând şi dezvoltând multe niveluri de activitate umană şi creând spaţiul cibernetic ca mediu global care nu poate exista în absenţa lui.

Statele şi dreptul internaţional nu au putut să se adapteze cu uşurinţă la evoluţia dinamică a tehnologiei şi să reacţioneze prin reglementarea tuturor problemelor legate de utilizarea şi mijloacele de comunicare ale acesteia. În acest sens, reacţia companiilor private, direct implicate şi interesate de acest domeniu şi adesea în afara contribuţiei şi sprijinului statelor a fost mai promptă în aşa fel încât

[1] Lector univ. dr., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iași, e-mail: carmen.moldovan@uaic.ro

paradigma normativă în reglementarea acestui mediu a trecut de la controlul exclusiv al statelor pentru a deveni un interesul mai multor părţi interesate.

Totuşi, scopul de a asigura aplicarea efectivă a normelor de drept internaţional în spaţiul cibernetic şi, în acelaşi timp, securitatea utilizatorilor acestuia se poate dovedi necesar în anumite contexte, dar nu poate justifica mijloace autoritare.

Prezenta lucrare îşi propune să analizeze dintr-o perspectivă critică, teoretică şi practică, ideea de suveranitate cibernetică (*cybersovereignty*). Spre deosebire de alte domenii ale dreptului internaţional, operaţiunile cibernetice reprezintă o formă relativ nouă de relaţii ale statelor, iar spaţiul cibernetic este considerat o zonă „gri" a dreptului internaţional, aparent în mare măsură neexploatată de state, din care dreptul internaţional nu poate fi exclus, însă se impune luarea în considerare a regulilor şi principiilor acestuia raportat la caracteristicile *Cyberspace* (denumire ce va fi folosită în cuprinsul prezentei lucrări pentru a desemna spaţiul cibernetic).

Evoluţiile recente de la nivelul Naţiunilor Unite constând în raporturile grupurilor de lucru special create – UN Group of Experts şi UN Open-ended Working Group – pe tema aplicării dreptului internaţional în *Cyberspace* au subliniat că dreptul internaţional este aplicabil fără a furniza detalii şi fără a preciza care sunt consecinţele juridice ale acestei constatări. În scopul acestei lucrări, termenul de suveranitate cibernetică se referă la aplicarea principiului suveranităţii statului în spaţiul cibernetic.

Există o asimetrie între crearea şi dinamica constantă a evoluţiei *Cyberspace* şi dezvoltarea unor reguli specifice drept internaţional în acest domeniu. Lacunele normative pot părea semnificative, iar necesitatea de a le acoperi este una reală şi poate avea consecinţe inclusiv asupra instituţiei răspunderii statului pentru fapte ilicite. Obiectivul prezentei lucrări este de a demonstra că aplicarea sensului teritorial clasic al suveranităţii în *Cyberspace* este incompatibilă cu trăsăturile spaţiului cibernetic ca mediu global şi cele două concepte pot fi reconciliate doar dacă statele acceptă o interpretare evolutivă a aplicării suveranităţii în acest mediu.

1. Cybersovereignty – concept şi implicaţii

Ideea de suveranitate cibernetică ce presupune crearea şi controlul asupra unui „ciberspaţiu naţional"[2], reglementat de legile interne ale unui stat este o manifestare a autoritarismului ce urmăreşte justificarea preluării controlului deplin asupra acestui mediu şi asupra internetului şi separarea acestora de reţeaua globală, ceea ce este contrar înseşi esenţei lor. O astfel de abordare este prezentată ca o

[2] M. Mueller, *Sovereignty and Cyberspace: Institutions and Internet governance*, Essay presented at the 5th Annual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana October 3rd 2018, [Online] la http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/10410/5th-Ostrom-lecture-DLC.pdf?sequence=1&isAllowed=y, accesat 10.10.2021.

alternativă la hegemonia Statelor Unite în *Cyberspace* ca spaţiu global[3] şi ca mijloc de a asigura principiul egalităţii între state ţinând cont de faptul că există diferenţe semnificative în ceea ce priveşte accesul real la *Cyberspace* din cauza nivelului tehnologic de dezvoltare inegal, rezultatul fiind un mediu fragmentat.

Această afirmaţie nu poate fi privită ca un argument pertinent având în vedere exact gradul de dezvoltare tehnologică, este puţin probabil ca ţările mai puţin dezvoltate să poată asigura efectiv securitatea reţelei lor cibernetice naţional, invocarea unor astfel de motive subliniază că problema reglementărilor în mediul *Cyberspace* este un instrument al rivalităţii geopolitice[4].

Cyberspace este caracterizat uneori ca haotic, anarhic[5] şi asimetric în raport cu resursele şi capacităţile celor care participă la diferite operaţiuni[6] pentru a justifica ideea unei suveranităţi cibernetice a statului care îşi protejează interesele în raport cu alte state, însă afirmarea acestui principiu nu rezolvă toate problemele ulterioare: răspunderea statului, consecinţe asupra intereselor şi drepturilor persoanelor private şi a actorilor nestatali.

Oricât de neclară ar fi la acest moment întinderea şi conţinutul principiilor aplicabile în acest mediu, caracterizarea ca anarhică nu este una satisfăcătoare. Caracteristici precum complexitatea, diversitatea utilizatorilor (state, actori nestatali, companii private, persoane private) au determinat crearea mai multor niveluri şi diferite tipuri de relaţii între utilizatorii săi, în funcţie de calitatea acestora şi de natura raporturilor create. Este întemeiată opinia potrivit căreia poate fi, din punct de vedere tehnic şi juridic, secţionat în mai multe părţi: reţele publice accesibile tuturor şi nelimitate de frontiere interne, cu acces liber; reţele teritoriale precum intranet-uri militare sau reţele guvernamentale cu acces limitat; reţele exclusive – pentru servicii de e-guvernare, afaceri, finanţe – accesul este limitat la persoanele autorizate[7]. Conceptul *cybersovereignty* nu ia în considerare aceste aspecte. Din aceste motive, termenul poate fi considerat inexact sau greşit pentru că principiul suveranităţii, care este piatra de temelie a dreptului internaţional, nu poate fi transferat pe deplin în *Cyberspace*. Noţiunea de suveranitate teritorială în spaţiul cibernetic trebuie aplicată în mod restrictiv, doar în raport cu elementele infrastructurii IT&C de pe teritoriul statului. Totodată, interpretarea

[3] Y. Shen, *Cyber Sovereignty and the Governance of Global Cyberspace*, Chin. Polit. Sci. Rev. (2016) 1:81–93, p. 82.

[4] H. Moynihan, *Power Politics Could Impede Progress on Responsible Regulation of Cyberspace,* 3 December 2019, [Online] la https://www.chathamhouse.org/expert/comment/power-politics-could-impede-progress-responsible-regulation-cyberspace, accesat 20.10.2021.

[5] S. Arsène, *Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order?* in China Perspectives 2016/2 | 2016 What Kind of International Order Does China Want, p. 28, https://doi.org/10.4000/chinaperspectives.6973.

[6] Y. Shen, *op. cit.,* p. 84.

[7] J. Zeng, T. Stevens, Y. Chen, *China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'*, Politics & Policy, Volume 45, No. 3, 2017, pp. 432-464, 451, https://doi.org/10.1111/polp.12202.

domeniului de aplicare a acestui principiu ar trebui făcută ţinând cont de evoluţia termenilor şi a relaţiilor reglementate de dreptul internaţional public pentru a acoperi decalajul în reglementarea comportamentului statelor în acest mediu.

2. Implicaţii ale caracterului sui generis al Cyberspace

Nu există consens între state cu privire la reglementarea *Cyberspace* sau chiar cu privire la înţelegerea funcţionării acestuia în acest mediu complex, a cărui definire şi caracteristici provin din literatura science-fiction, din *Neuromantul* scris de Wiliam Gibson. Aceste aspecte nu vor fi abordate în cuprinsul prezentei lucrări deoarece au făcut obiectul unor alte studii şi articole[8]. O definiţie standard sau obiectivă a acestui mediu lipseşte[9] astfel că termenul este utilizat în general în privinţa oricăror aspecte ale utilizării reţelelor de computere şi internet şi pentru a descrie legăturile cu reţelele şi computerele[10] mai ales în domeniul securităţii[11]. Lipsa unei definiţii unice nu este însă de natură a împiedica aplicarea regulilor şi principiilor dreptului internaţional în acest mediu şi în privinţa conduitei statelor[12].

Spre deosebire de teritoriul statului, care are o dimensiune fizică şi materială unde este aplicabil principiul suveranităţii, *Cyberspace* este în întregime creaţia omului[13] şi constituie o reţea globală complexă, un spaţiu logic, nelimitat, imperceptibil, nematerializat, dependent de timp[14], în continuă schimbare, un

[8] C. Moldovan, *Blurred lines in defining the conduct of States in Cyberspace. A critical analysis on the cyber sovereignty and impact over free access to information*, presented at European Society of International Law Kraków-Leiden Online Symposium on 'Exploring the Frontiers of International Law in Cyberspace', 4 December 2020; C. Moldovan, *Limits of International Law in a limitless Cyberspace. Challenges and uncertainties*, în Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" din Iaşi, Tomul LXVI/Supliment, Ştiinţe juridice, 2020, pp. 315-326, [Online] la http://pub.law.uaic.ro/files/articole/2020/2020_i_bis/21._moldovan_dip_cyberspace.pdf, accesat 20.10.2021; C. Moldovan, *Are there any limits to the rights of States in Cyberspace? An analysis from the perspective of International Law*, presented at the 13th Biennial International Conference organised by the Faculty of Law of the West University of Timişoara, 6-7 November 2020.

[9] R. Ottis, P. Lorents, *Cyberspace: Definition and Implications*, in Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April 2010, [Online] la https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/, accesat 20.10.2021.

[10] *Ibidem.*

[11] E. Donahoe, *The Need for a Paradigm Shift on Digital Security*, eds. Fen Osler Hampson and Michael Sulmeyer, *Getting beyond Norms New Approaches to International Cyber Security Challenges* Special Report, Centre for International Governance Innovation, 2017, p. 31

[12] C. Moldovan, *op. cit., Limits* .... 2020, p. 318-319.

[13] M. Baezner, P. Robin, *Trend Analysis: Cyber Sovereignty*, Risk and Resilience Team Center for Security Studies (CSS) ETH Zürich, 2018, p. 8.

[14] R. Ottis, P. Lorents, *op. cit.*

sistem informaţional interconectat creat de actori nestatali, fără frontiere[15], ce este legat de teritoriul fizic prin infrastructură fără de care nu poate exista[16].

Toate aceste elemente descriu un fenomen *sui generis*[17], probabil una dintre cele mai mari creaţii ale umanităţii din prezent, un spaţiu civil şi militar deopotrivă ce nu poate fi e supus controlului exclusiv al statelor, deoarece nu poate fi plasat sub suveranitatea statului[18].

Caracteristicile speciale aseamănă acest mediu cu cele în care statele nu îşi exercită jurisdicţia exclusivă sau se bucură de prerogative speciale, cum ar fi marea liberă sau spaţiul cosmic ce au regim juridic special.

Complexitatea Cyberspace şi trăsăturile sale explică motivele furnizării unei definiţii general acceptate sau incluse în cuprinsul unui tratat internaţional. O astfel de sarcină se poate dovedi nu doar dificilă, ci şi imposibilă (sens în care amintim lipsa reglementărilor cu caracter obligatoriu în acest domeniu, cu excepţia *Convenţiei de la Budapesta privind criminalitatea informatică*[19], adoptată în cadrul Consiliului Europei). În acest context, crearea la nivelul Naţiunilor Unite a grupurilor de lucru specializate – UNGGE *(the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security)* şi OEWG *(Open-ended working group on developments in the field of information and telecommunications in the context of international security)*[20] – reprezintă o încercare de a clarifica aplicabilitatea regulilor dreptului internaţional public. Începând cu anul 2013[21] până în prezent, concluziilor ambele

[15] K. Nyman Metcalf, *Legal View on Outer Space and Cyberspace: Similarities and Differences*, Tallinn Paper No. 10, 2018, p. 2, [Online] la https://ccdcoe.org/uploads/2018/10/Tallinn-Paper_10_2018.pdf, accesat 12.10.2021.

[16] Y. Shen, *op. cit.*, p. 83.

[17] D. Broeders, L. Adamson, R. Creemers, *Coalition of the unwilling? Chinese and Russian perspectives on cyberspace,* in The Hague Program For Cyber Norms Policy Brief. November 2019, p. 2, [Online] la https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 3493600, accesat 29.11.2021.

[18] W. Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, in 4th International Conference on Cyber Conflict C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), NATO CCDCOE Publications, 2012, p. 8.

[19] Council of Europe, *Convention on Cybercrime*, 23.XI.2001, ETS No.185.

[20] UNODA, *Fact Sheet - Developments in the field of information and telecommunications in the context of International Security*, 2019, [Online] la https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf, accesat 21.10.2021.

[21] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* para. 19, U.N. Doc. A/68/98, June 24, 2013, [Online] la http://undocs.org/A/68/98, accesat 21.10.2021; United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 2015, [Online] la https://undocs.org/A/ 70/174, accesat 21.10.2021; United Nations General Assembly (2018), *Resolution adopted by the General Assembly on 22 December 2018 on "Advancing responsible State behaviour in Cyberspace in the context of international security"*, UN Doc A/RES/73/266, [Online] la

grupuri au fost în sensul aplicării dreptului internaţional pentru conduita statelor în acest mediu, însă un rol esenţial în lămurirea efectelor acestora revine statelor, care au exprimat oficial puncte de vedere fie în cadrul grupurilor de lucru, fie prin declaraţii speciale în această privinţă.

Normele privind comportamentul responsabil al statelor în *Cyberspace*, identificate prin documentele celor două grupuri de lucru, au fost considerate norme acceptate voluntar de către state (*voluntary norms*)[22], exprimare ce este ambiguă şi conturează lipsa forţei juridice obligatorii şi creează incertitudine inclusiv în ceea ce priveşte aplicarea principiului suveranităţii în acest mediu.

Concluzii din luna iulie 2020 ale OEWG subliniază rolul esenţial al Raportului din 2015 adoptat în cadrul UNGGE, care susţine necesitatea implementării normelor voluntare identificate pentru a asigura caracterul public al internetului, prin raportare la obligaţia de respectare a drepturilor fundamentale[23]. Un alt document, din octombrie 2020, denumit *The future of discussions on ICTs and Cyberspace at the UN*[24] propune stabilirea unui *Program de acţiune pentru promovarea comportamentului responsabil al statului în spaţiul cybernetic (Programme of Action for advancing responsible State behaviour in Cyberspace),* în vederea încetării discuţiilor în două niveluri (GGE şi OEWG) şi a stabilirii unui forum permanent în cadrul Naţiunilor Unite pentru analiza utilizării tehnologiilor de informaţii şi comunicare de către state în contextul securităţii internaţionale, luând în considerare constatările făcute de cele două grupuri de lucru.

3. Caracteristicile principiului suveranităţii statului

Pentru a justifica ideea de suveranitate a statului în Cyberspace, se foloseşte principiul suveranităţii teritoriale. Deşi principiul a fost consacrat cu multă vreme în urmă, dreptul internaţional nu conţine o definiţie exhaustivă a acestuia, astfel încât identificarea elementelor şi semnificaţiei acesteia este relevantă pentru

https://undocs.org/en/A/RES/73/266, accesat 21.10.2021; United Nations General Assembly, Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, 10 March 2021, *Final Substantive Report,* A/AC.290/2021/CRP.2, [Online] la https://ict4peace.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf, accesat 21.10.2021.

[22] E. Tikk, M. Kerttunen, *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, in Cyber Policy Institute, 2017, p. 14.

[23] Statements by the Republic of Finland Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security Virtual Informal Consultations 19 June and 2 July 2020, Statement 2 delivered 2 July 2020, [Online] la https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-finland-19-june-and-2-july-2020.pdf, accesat 10.09.2021.

[24] OEWG, *The future of discussions on ICTs and Cyberspace at the UN*, [Online] la https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf, accesat 10.10.2021.

analiza aplicabilităţii acestuia în mediul analizat şi pentru identificarea limitelor sale, cum sunt jurisdicţia şi imunităţile statului. Complexitatea conceptului este amplificată de faptul că sensul modern al suveranităţii se referă la popoarele din cadrul statului, nu exclusiv la statul însuşi ca entitate juridică[25].

Suveranitatea ca principiu datează din secolul al XVI-lea şi este unul dintre conceptele dezvoltate după Pacea de la Westfalia din 1648[26]. Sistemul Westfalian considera că statele deţin suveranitate asupra teritoriilor şi afacerilor interne ale acestora fără intervenţia altor state.

Principiul suveranităţii statului este unul dintre principiile fundamentale ale dreptului internaţional, consacrat în articolul 2 paragraful 1 din Carta Naţiunilor Unite[27] şi instrumentele juridice ulterioare (*Declaraţia privind principiile dreptului internaţional, relaţiile de prietenie şi cooperarea între state în conformitate cu Carta Naţiunilor Unite[28]*, *Actul Final Helsinki[29]*, *Carta de la Paris pentru o nouă Europă[30]*) au menţionat, de asemenea, acest principiu şi valoarea sa ridicată pentru dreptul internaţional şi au stabilit legături între acesta şi alte principii fundamentale precum neintervenţia, autodeterminarea, integritatea teritorială şi soluţionarea paşnică a diferendelor[31].

Dintr-o perspectivă teritorială, suveranitatea statului şi alte principii fundamentale ale dreptului internaţional se aplică tuturor componentelor teritoriului unui stat aflat în interiorul graniţelor sale (terestre, maritime, aeriene) în care acesta se bucură de o exclusivitate incontestabilă şi plenitudine de competenţă. Toate elementele suveranităţii statului se referă şi sunt analizate în legătură cu teritoriul fizic al statului în funcţie de stadiul de evoluţie al regulilor şi conceptelor de drept internaţional. Suveranitatea, atribut esenţial al statului atât la nivel internaţional cât şi intern[32], descrie competenţele statelor şi prezintă de fapt sensuri

---

[25] S. Besson, *Sovereignty, International Law and Democracy,* in The European Journal of International Law, Vol. 22 no. 2, 2011, p. 383, https://doi.org/10.1093/ejil/chr029.

[26] A. Osiander, *Sovereignty, International Relations, and the Westphalian Myth*, in International Organization, vol. 55, no. 2, 2001, pp. 251–287, DOI: https://doi.org/10.1162/ 00208180151140577.

[27] Articolul 2 paragraful 1 al cartei Naţiunilor Unite prevede: „1. Organizaţia este întemeiată pe principiul egalităţii suverane a tuturor Membrilor ei".

[28] United Nations General Assembly Resolution 2625 (XXV), adopted on 24 October 1970, A/RES/26/25 (XXV), *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations (24 October 1970).*

[29] Organization for Security and Co-operation in Europe, Helsinki Final Act, August 1975, [Online] la https://www.osce.org/helsinki-final-act, accesat 12.10.2021.

[30] Organization for Security and Co-operation in Europe, Charter of Paris for a New Europe, 21 November 1990, [Online] la https://www.osce.org/mc/39516, accesat 12.10.2021.

[31] H. Steinberger, "Sovereignty", în *Encyclopedia of Public International Law,* Volume four, North-Holland, Elsevier, 2000, p. 513.

[32] J. Combacau, S. Sur, *Droit international public,* 12e edition, LGDJ 2016, p. 238; M. Bennouna, *Le droit international entre la lettre et l`esprit. Cours général de droit international public*, (Collected Courses of the Hague Academy of International Law, Tome 383, Brill /Nijhoff), 2016, p. 42.

multiple, este indivizibilă, exclusivă, inalienabilă şi reprezintă o garanţie a derulării relaţiilor dintre state[33], bazate pe independenţă şi lipsa de subordonare a unui stat faţă de celelalte[34].

În analiza conţinutului şi a implicaţiilor principiului suveranităţii, multe lucrări academice au ca reper concluziile din cauza *Insula Palmas*[35], ce a analizat dimensiunea teritorială a suveranităţii astfel:

„*Suveranitatea teritorială (...), implică dreptul exclusiv al unui stat a-şi face publice activităţile. Acest drept are corolar o îndatorire: obligaţia de a proteja în interiorul teritoriului drepturile altor state, în special dreptul lor la integritate şi inviolabilitate în timp de pace şi război, împreună cu drepturile pe care fiecare stat le poate pretinde pentru cetăţenii săi pe teritoriul străin*"[36]. În acelaşi timp, trebuie subliniat că hotărârea arbitrală a avut în vedere natura dinamică a conceptului de suveranitate, şi a menţionat:

„*Manifestările de suveranitate teritorială îmbracă, este adevărat, forme diferite, în funcţie de condiţiile de timp şi de loc*"[37].

Această concluzie poate fi folosită pentru a justifica interpretarea restrictivă a suveranităţii statului în *Cyberspace.*

Suveranitatea se bazează pe ideea exercitării controlului sau a unei manifestări de autoritate pe un anumit teritoriu[38] al statului şi a altor spaţii cu statut juridic special şi include controlul asupra tuturor persoanelor de pe teritoriu[39], care are semnificaţia exercitării competenţei (competenţă prescriptivă, competenţă de a judeca, competenţă de executare). Sensul principiului suveranităţii este rezultatul evoluţiei şi are o semnificaţie diferită de cea pe care a prezentat-o în secolele al XVI-lea şi al XVII-lea când a apărut ca urmare a intenţiei monarhiilor europene de a-şi consolida poziţia în raport cu biserica[40].

Transpunerea în *Cyberspace* a ideii de suveranitate având conţinutul anterior descris, are ca efect exercitarea controlului în acest mediu asupra elementelor care susţin suveranitatea. În acest sens, lucrările grupurilor din cadrul Naţiunilor Unite - GGE şi OEWG nu se referă la o idee abstractă de suveranitate, ci se raportează la infrastructura IT &C aparţinând statului sau situată pe teritoriul acestuia, abordare pe deplin compatibilă cu caracteristicile şi elementele suveranităţii.

---

[33] C. Moldovan, *Drept internațional public. Principii și instituții fundamentale*, Ediția a II-a, Editura Universul Juridic, București, 2019, p. 140.

[34] J. Crawford, *Brownlie's Principles of Public International Law,* Eighth Edition, Oxford University Press, 2012, p. 447.

[35] PCA, *Island of Palmas Case* (or Miangas), United States of America v. The Netherlands, Award of the Tribunal, 4 April 1928, [Online] la https://pcacases.com/web/sendAttach/714, accesat 20.10.2021.

[36] *Idem*, p. 9.

[37] *Ibidem.*

[38] ICJ, T*erritorial and Maritime Dispute* (Nicaragua v. Colombia) Judgment of 19 November 2012.

[39] A. Cassese, *International Law*, Second Edition, Oxford University Press, 2005, p. 49.

[40] M. Bennouna, *op. cit.,* p. 41.

4. Divergenţe şi confluenţe asupra suveranităţii cibernetice

Conceptul de suveranitate cibernetică a fost folosit pentru prima dată promovat intens de China şi include mai multe prerogative ale statului, conform legislaţiei naţionale, de a reglementa conduita persoanelor private în legătură cu folosirea internetului şi a datelor cu caracter personal pe teritoriul său, ca mijloc de protejare a spaţiului informaţional, în conformitate cu politica generală privind controlul internetului şi fluxul de date[41]. Statul chinez a iniţiat proiectul numit *The Golden Shield,* în 1996 şi l-a implementat în 2008[42]. Acesta este exemplul perfect, deoarece stabileşte controlul deplin al statului asupra informaţiilor şi accesului la informaţii.

Acelaşi tip de abordare este reflectată şi extinsă de legislaţia internă a Federaţiei Ruse care a adoptat în 2019 *„Legea suverană a internetului"*[43] ce stabileşte cadrul legal pentru controlul asupra internetului între frontierele acesteia[44]. Federaţia Rusă a susţinut crearea unei reţele naţionale proprii pentru care a fost deja făcute teste şi utilizatorii nu au întâmpinat probleme sau nici măcar nu şi-au dat seama că au intervenit schimbări. Anterior, în decembrie 2016, Preşedintele Federaţiei Ruse a aprobat *doctrina securităţii informaţionale* care presupune crearea internetului şi mediului cibernetic naţional, precum şi separarea acestuia de spaţiul cibernetic internaţional[45].

Justificarea dată de preşedintele rus este că aceasta reprezintă o măsură de securitate pentru protejarea statului în cazul unei „urgenţe sau ameninţări străine precum un atac cibernetic"[46]. Potrivit legii, statul are prerogativa de a controla internetul prin infrastructura instituită în Rusia şi de a crea un sistem propriu de nume pentru domeniile de internet. Din perspectiva consecinţelor sale, o astfel de măsură constituie deconectarea reţelei de infrastructură rusă de la reţeaua globală şi în mod practic, constituie instaurarea cenzurii pentru utilizatorii săi.

O astfel de posibilitate tehnică poate fi pusă în practică fără mare dificultate şi ar putea fi văzută ca o manifestare a jurisdicţiei teritoriale[47]. Totuşi, situaţia în care toate statele, în numele suveranităţii cibernetice, şi-ar crea şi izola reţeaua

[41] D. Broeders, L. Adamson, R. Creemers, *op. cit.*, p. 2.

[42] S. Chandel, Z. Jingji, Y. Yunnan, S. Jingyao, Z. Zhipeng, *The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall*, în 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2019, p. 111-119, DOI: https://doi.org/10.1109/CyberC.2019.00027.

[43] A. Epifanova, *Deciphering Russia's "Sovereign Internet Law" Tightening Control and Accelerating the Splinternet,* German Council on Foreign Relations DGAP Analysis, No 2 January 2020, [Online] la https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf, accesat 12.10.2021.

[44] *Ibidem.*

[45] [Online] la https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html, accesat 10.11.2021.

[46] [Online] la https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html, accesat 10.11.2021.

[47] W.H. Heintschel von Heinegg, *op. cit.,* p. 9.

naţională, nu ar mai corespunde ideii de reţea internaţională globală aşa cum o cunoaştem şi o folosim astăzi şi ar sacrifica cu siguranţă internetul[48]. Ar fi doar o extindere a teritoriului naţional, controlat în întregime de stat, inclusiv controlul asupra datelor, fluxului de date, utilizatorilor, parametrilor tehnici şi caracteristicile generale ale acestui spaţiu.

La polul opus, o abordare diferită, mult mai temperată calitativ şi cantitativ aparţine Franţei şi a fost exprimată în *Cartea Albă a Apărării şi Securităţii Naţionale* din 2013[49], care se concentrează asupra necesităţii de a proteja integritatea statului şi a infrastructurii în anumite cazuri care ar echivala cu un atac armat. Această viziune a fost extinsă în acte ulterioare precum *Strategia internaţională* din 2017[50] şi *Analiza strategică* din 2018 *a apărării cibernetice*[51]. Aceasta din urmă afirmă că:

„(...) principiul suveranităţii se aplică spaţiului cibernetic. În acest sens, Franţa îşi reafirmă suveranitatea asupra infrastructurii tehnologiilor informaţiei şi comunicaţiilor, a persoanelor şi a activităţilor cibernetice situate pe teritoriul său, sub rezerva obligaţiilor sale legale internaţionale".

Franţa a dezvoltat un sistem naţional de definire şi calificare a acţiunilor care constituie un incident de securitate cibernetică. În stabilirea pragului unei încălcări de suveranitate, abordarea franceză se concentrează pe comportamentul în sine reprezentând pătrunderea sistemului IT&C, nu pe consecinţele produse.

Un alt exemplu de abordare globală asupra *Cyberspace* este reprezentat de Statele Unite ale Americii, care propune *Strategia naţională cibernetică* din 2018[52], axată pe ideea de mediu global şi deschis ce promovează:

> *„un cadru pentru comportamentul responsabil al statului în Cyberspace construit pe dreptul internaţional, aderarea la normele voluntare neobligatorii de comportament responsabil al statului, care se aplică în timp de pace şi luarea în considerare a măsurilor practice de consolidare a încrederii pentru a reduce*

[48] M. Mueller, *op. cit*., p. 5.

[49] Direction générale des relations internationales et de la stratégie (DGRIS)/Directorate General for International Relations and Strategy, *White Paper on Defence and National Security 2013*, [Online] la https://www.defense.gouv.fr/english/dgris/defence-policy/white-paper-2013/white-paper-2013, accesat 20.11.2021.

[50] French Foreign Policy, *Stratégie internationale de la France pour le numérique,* [Online] la https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy/https://www.ife.ee/en/international-strategy-for-digital/, accesat 20.11.2021.

[51] Secretary general on Defense and National Security (France), *Strategic review of cyber defence*, February 2018, [Online] la http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf, accesat 20.11.2021; F. Delerue, A. Géry, *France's Cyberdefense Strategic Review and International* Law, March 23, 2018, [Online] la https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law, accesat 20.11.2021.

[52] The White House, *National Cyber Strategy of the United States of America*, September 2018, p. 20, [Online] la https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, accesat 20.11.2021.

riscul de conflict care decurge din activitatea cibernetică rău intenţionată. Aceste principii ar trebui să formeze o bază pentru cooperarea statelor în scopul contracarării acţiunilor care nu sunt conforme cu acest cadru."

În 2021, a fost emis un Ordin executiv pentru îmbunătăţirea securităţii cibernetice naţionale, care se axează pe adoptarea de măsuri pentru protejarea mediului cibernetic, supus unor numeroase atacuri[53].

Regatul Unit a dezvoltat de asemenea, o strategie naţională de securitate cibernetică[54], a creat un centru naţional pentru securitate cibernetică[55] şi susţine aplicabilitatea suveranităţii ca principiu, considerând că nu există o regulă a suveranităţii în Cyberspace[56]. Din punct de vedere teoretic şi practic, diferenţele dintre cele două abordări ale suveranităţii: ca principiu şi ca regulă, nu sunt de fapt foarte clare şi eficacitatea lor poate să nu fie semnificativă, deoarece în fiecare caz există obligaţii internaţionale pentru state.

Poziţiile exprimate public de state cu privire la suveranitatea în Cyberspace pot fi foarte diferite în practică, ceea ce face dificilă argumentarea existenţei unei *opinio iuris* asupra modului în care aceasta se aplică, însă această situaţie nu înseamnă în mod necesar existenţa unui vid normativ[57].

Nu toate statele au exprimat puncte de vedere detaliate[58] cu privire la modalitatea în care dreptul internaţional se aplică în *Cyberspace*, însă tăcerea statelor sau poziţia lor ambiguă poate fi cea mai bună modalitate de a asigura aplicarea dreptului internaţional în spaţiul cibernetic.

Concluzii

Noţiunea de „suveranitate digitală" este una ambiguă, în ciuda eforturilor de a clarifica implicaţiile acesteia în *Cyberspac*e făcute la nivelul Naţiunilor Unite. Sunt

[53] The White House, *Executive Order On Improving the Nations`s Cybersecurity*, May 12, 2021, [Online] la https://www.whitehouse.gov/briefing-room/presidential-actions/ 2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, accesat 20.11.2021.

[54] Cabinet Office and National Security and Intelligence, *National Cyber Security Strategy 2016 to 2021*: progress so far, [Online] la https://www.gov.uk/ government/ publications/national-cyber-security-strategy-2016-to-2021-progress-so-far, accesat 20.11.2021.

[55] National Cyber Security Centre, [Online] la https://www.ncsc.gov.uk/section/about-ncsc/what-we-do, accesat 20.11.2021.

[56] UK Attorney General Jeremy Wright Speech, *Cyber and International Law in the 21st Century*, 23 May 2018, [Online] la https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century, accesat 21.11.2021.

[57] M. Tolppa O*verview of the UN OEWG developments: continuation of discussions on how International Lawapplies in cyberspace,* 2020, [Online] la https://ccdcoe.org/ library/publications/overview-of-un-oewg-developments-continuation-of-discussions-on-how-international-law-applies-in-cyberspace/, accesat 21.11.2021.

[58] O prezentare a poziţiilor statelor în cadrul sesiunilor OEWG poate fi consultată [Online] la https://www.un.org/disarmament/open-ended-working-group/, accesat 20.11.2021.

necesare eforturi suplimentare din partea statelor şi a organismelor internaţionale pentru a defini această noţiune şi a stabili conţinutul şi limitele sale, prin referire la principiul fundamental al suveranităţii statului.

Faptul că grupurile de lucru special create în cadrul Naţiunilor Unite nu au reuşit să dezvolte norme de drept internaţional prin mijloace şi canale diplomatice subliniază această necesitate. Deşi activitatea şi constatările sale au fost incomplete şi uneori criticate, Naţiunile Unite rămâne cel mai potrivit şi legitim forum deschis tuturor statelor pentru a discuta toate tipurile de probleme legate de acest mediu, iar dezbaterile din Adunarea Generală pot oferi premisele *opinio juris* asupra comportamentului statelor şi a unei guvernări globale în Cyberspace.

Conceptul de „suveranitate cibernetică" se opune ideii de guvernanţă globală şi nu ţine cont de interesele tuturor părţilor interesate (*mutistakeholders*), cum ar fi companiile private şi persoanele private. Exercitarea suveranităţii statului în acest mediu este limitată şi nu are aceeaşi sferă ca şi teritoriul fizic al statului. O abordare echilibrată în această privinţă ar fi luarea în considerare a unei semnificaţii diferite, raportat la elementele infrastructurii fizice de care depinde existenţa *Cyberspace*, urmând a fi clarificate noţiuni precum jurisdicţia statului, efectele extrateritoriale ori încălcarea suveranităţii în spaţiul virtual.

Referinţe

Arsène S., *Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order?* in China Perspectives 2016/2 | 2016 What Kind of International Order Does China Want, p. 28, https://doi.org/10.4000/chinaperspectives.6973

Baezner M., Robin P., *Trend Analysis: Cyber Sovereignty,* Risk and Resilience Team Center for Security Studies (CSS) ETH Zürich, 2018

Bennouna M., *Le droit international entre la lettre et l`esprit. Cours général de droit international public*, (Collected Courses of the Hague Academy of International Law, Tome 383, Brill /Nijhoff), 2016

Besson S., *Sovereignty, International Law and Democracy,* in The European Journal of International Law Vol. 22 no. 2, 2011, https://doi.org/10.1093/ejil/chr029.

Broeders D., Adamson L., Creemers R., *Coalition of the unwilling? Chinese and Russian perspectives on cyberspace,* in The Hague Program For Cyber Norms Policy Brief, November 2019

Cabinet Office and National Security and Intelligence, *National Cyber Security Strategy 2016 to 2021*: progress so far, 2021

Cassese A., *International Law*, Second Edition, Oxford University Press, 2005

Chandel S., Jingji Z., Yunnan Y., Jingyao S., Zhipeng Z., *The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall*, în 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2019, https://doi.org/10.1109/CyberC.2019.00027

Combacau J., Sur S., *Droit international public,* 12e edition, LGDJ, 2016

Council of Europe, *Convention on Cybercrime*, 23.XI.2001, ETS No.185

Crawford J., *Brownlie's Principles of Public International Law,* Eighth Edition, Oxford University Press, 2012

Delerue F., Géry A., *France's Cyberdefense Strategic Review and International* Law, March 23, 2018

Direction générale des relations internationales et de la stratégie (DGRIS)/Directorate General for International Relations and Strategy, *White Paper on Defence and National Security*, 2013

Donahoe E., *The Need for a Paradigm Shift on Digital Security*, eds. Fen Osler Hampson and Michael Sulmeyer, *Getting beyond Norms New Approaches to International Cyber Security Challenges* Special Report, Centre for International Governance Innovation, 2017

Epifanova A., *Deciphering Russia's „Sovereign Internet Law" Tightening Control and Accelerating the Splinternet,* German Council on Foreign Relations DGAP Analysis, no 2/2020

Heintschel von Heinegg W., *Legal Implications of Territorial Sovereignty in Cyberspace,* in 4th International Conference on Cyber Conflict C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), NATO CCDCOE Publications, 2012

Moldovan C., *Drept internaţional public. Principii şi instituţii fundamentale*, Ediţia a II-a, Editura Universul Juridic, Bucureşti, 2019

Moldovan C., *Blurred lines in defining the conduct of States in Cyberspace. A critical analysis on the cyber sovereignty and impact over free access to information,* presented at European Society of International Law Kraków-Leiden Online Symposium on 'Exploring the Frontiers of International Law in Cyberspace', 4 December 2020

Moldovan C., *Limits of International Law in a limitless Cyberspace. Challenges and uncertainties*, în Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" din Iaşi, Tomul LXVI/Supliment, Ştiinţe juridice, 2020

Moldovan C., *Are there any limits to the rights of States in Cyberspace? An analysis from the perspective of International Law,* presented at the 13th Biennial International Conference organised by the Faculty of Law of the West University of Timişoara, 6-7 November 2020

Moynihan H., *Power Politics Could Impede Progress on Responsible Regulation of Cyberspace,* December 3rd 2019

Mueller M., *Sovereignty and Cyberspace: Institutions and Internet governance,* Essay presented at the 5th Annual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana October 3rd 2018

Nyman Metcalf K., *Legal View on Outer Space and Cyberspace: Similarities and Difference*, Tallinn Paper, no. 10/2018

Ottis R., Lorents P., *Cyberspace: Definition and Implications*, in Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April 2010

OEWG, *The future of discussions on ICTs and Cyberspace at the UN,* on-line.

Organization for Security and Co-operation in Europe, Helsinki Final Act, August 1975, on-line

Osiander A., *Sovereignty, International Relations, and the Westphalian Myth*, in International Organization, vol. 55, no. 2, 2001, DOI: https://doi.org/10.1162/00208180151140577

PCA, *Island of Palmas Case* (or Miangas), United States of America v. The Netherlands, Award of the Tribunal, 4 April 1928

Shen Y., *Cyber Sovereignty and the Governance of Global Cyberspace*, Chin. Polit. Sci. Rev. 1/2016, pp. 81–93

Steinberger H., "Sovereignty", în *Encyclopedia of Public International Law* (Volume four, North-Holland, Elsevier, 2000

Tikk E., Kerttunen M., *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, in Cyber Policy Institute, 2017

Tolppa M., O*verview of the UN OEWG developments: continuation of discussions on how International Law applies in cyberspace*, 2020, on-line

United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* para. 19, U.N. Doc. A/68/98, June 24th, 2013

United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* A/70/174, 2015

United Nations General Assembly,"*Resolution adopted by the General Assembly on 22 December 2018 on „Advancing responsible State behaviour in Cyberspace in the context of international security"*, UN Doc A/RES/73/266, 2018

United Nations General Assembly, Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, *Final Substantive Report,* A/AC.290/2021/CRP, 2021

United Nations General Assembly Resolution 2625 (XXV), adopted on 24 October 1970, A/RES/26/25 (XXV), *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, 1970

UNODA, *Fact Sheet - Developments in the field of information and telecommunications in the context of International Security*, 2019, on-line

The White House, *National Cyber Strategy of the United States of America*, September 2018

The White House, *Executive Order On Improving the Nations`s Cybersecurity*, May 12, 2021, on-line

UK Attorney General Jeremy Wright Speech, *Cyber and International Law in the 21st Century*, 23 May 2018

Zeng J., Stevens T., Chen Y., *China's Solution to Global Cyber Governance: Unpacking the Domestic* Discourse of 'Internet Sovereignty', Politics & Policy, Volume 45, no. 3/2017, https://doi.org/10.1111/polp.12202.

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-20

Provocări tehnologice în crearea standardelor pentru analiza amprentelor digitale

Technological Challenges in Creating Standards for Fingerprint Analysis

Ancuţa Elena Franţ[1]

Rezumat: Este cunoscut faptul că analiza amprentelor este o metodă care poate duce la identificarea corectă a unei persoane. Este mai puţin cunoscut faptul că acurateţea acestei metode este pusă în pericol, atunci când se utilizează tehnologia digitală pentru a stoca şi a compara informaţii cu privire la amprente. Utilizarea tehnologiei în analiza amprentelor este foarte importantă, deoarece permite diverse activităţi care sunt vitale pentru o anchetă penală, de exemplu comparaţia între o anumită amprentă, găsită la locul crimei, şi amprentele stocate în baze de date. Cu toate acestea, stocarea amprentelor prin utilizarea inteligenţei artificiale nu este o sarcină simplă, deoarece informaţiile trebuie protejate de potenţiale ameninţări. O modalitate simplă de a proteja informaţiile referitoare la amprente este de a cripta informaţiile, dar aceasta înseamnă că, atunci când informaţiile sunt transferate, receptorul trebuie să aibă cheia corespunzătoare pentru a decripta informaţiile. Acest lucru duce la necesitatea unui algoritm standard, care trebuie utilizat atât de expeditor, cât şi de receptor. Această lucrare analizează provocările creării unui astfel de algoritm standard şi evaluează implicaţiile standardizării în ceea ce priveşte utilizarea amprentelor în identificarea criminalistică.

Cuvinte-cheie: amprentă digitală; standardizare; investigaţie penală; algoritm

Abstract: It is widely known that the analysis of fingerprints is a method which can lead to the correct identification of a person. It is lesser known that the accuracy of this method is endangered, when it comes to using digital technology, in order to store and compare information regarding fingerprints. The use of digital technology in analysing fingerprints is very important, because it enables various activities which are vital for a criminal investigation, for example the comparison between a certain fingerprint, found at crime scene, with the fingerprints which are stored in databases. However, storing fingerprints in a digital form is not a simple task, as the information must be protected from potential threats. A simple way to protect the information regarding fingerprints is to encrypt the information, but this means that, when information is transferred, the receptor must have the appropriate key, in order to decrypt the information. This leads to the necessity of a standard algorithm, which must be used by both the sender and the receiver. This paper

[1] Lector univ. dr., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iași, e-mail: ancuta.frant@uaic.ro.

analyses the challenges of creating such a standard algorithm and assesses the implications of standardization in fingerprinting.

Keywords: fingerprint; standardization; criminal investigation; algorithm

1. Importanţa tehnologiei în utilizarea amprentelor digitale

Folosirea amprentele digitale este, în esenţă, o latură a biometriei, care reprezintă ştiinţa identificării indivizilor pe baza caracteristicilor biologice[2]. Parametrii biometrici care pot fi utilizaţi pentru identificare sunt multipli şi includ: amprentele digitale, geometria mâinii, reţeaua vaselor de sânge subcutanate, trăsăturile feţei, irisul, amprenta vocală[3].

Analiza amprentelor digitale reprezintă o metodă de identificare criminalistică de mare acurateţe. Utilizarea analizei amprentelor nu se limitează, însă doar la domeniul investigaţiilor penale. Fiind o metodă de identificare a persoanelor, amprentele prezintă potenţial de utilizare în orice domeniu în care este necesară autentificarea indivizilor, de exemplu pentru a accesa un computer, telefonul mobil, un automat bancar, maşina sau chiar casa. Practic, utilizarea amprentelor asigură o securitate sporită, permiţând doar persoanelor autorizate să aibă acces în diferite situaţii, dintre care cele mai frecvente se referă la utilizarea anumitor bunuri. În demersul de utilizare a amprentelor digitale în diferite domenii, multe dintre ele de natură comercială, este absolut necesară folosirea tehnologiei[4].

În ceea ce priveşte analiza amprentelor în scopul identificării criminalistice, tehnologia permite stocarea unui număr foarte mare de amprente şi compararea relativ rapidă a unei amprente găsită la faţa locului cu amprentele din bazele de bate. De asemenea, tehnologia permite desfăşurarea cu succes a cooperării între organele de poliţie, la nivel naţional şi internaţional, în scopul asigurării operativităţii în acţiunile de combatere şi prevenire a criminalităţii naţionale şi internaţionale. Un exemplu de utilizare cu succes a tehnologiei pentru folosirea amprentelor în anchetele penale îl reprezintă programele de tip AFIS[5]. Practic, fără utilizarea tehnologiei, analiza amprentelor în scop criminalistic s-ar face cu mare dificultate, mai ales în contextul actual al dezvoltării la scară foarte largă a criminalităţii transfrontaliere; aceasta ar umbri potenţialul extraordinar de identificare pe care îl prezintă amprentele digitale.

---

[2] A. Jain, R. Bolle, S. Pankanti, *Introduction to Biometrics*, în A. Jain, Bolle R., Pankanti S. (editori), *Biometrics*, Springer, Boston, MA, 1996, pp. 1-41, [Online] la https://doi.org/10.1007/0-306-47044-6_1, accesat 17.11.2021.

[3] T. Frater, *Standards for Fingerprint Identification*, [Online] la http://www.sis.pitt.edu/mbsclass/standards/frater/intro.htm, accesat 3.12.2021.

[4] Pentru detalii, a se vedea L. O'Gorman, *An overview of fingerprint verification technologies*, în Information Security Technical Report, Vol. 3, Nr. 1/1998, pp. 21-32, [Online] la https://doi.org/10.1016/S1363-4127(98)80015-0, accesat 17.11.2021.

[5] Pentru detalii, a se vedea A. Jain, S. Pankanti, *Automated Fingerprint Identification and Imaging Systems*, în H. C. Lee, R. E. Gaensslen (editori), *Advances in Fingerprint Technology*, second edition, CRC Press, Boca Raton, 2001, pp. 285-336.

În privinţa utilizării amprentelor în scopul permiterii accesului la anumite bunuri sau servicii, tehnologia este, de asemenea, indispensabilă. Autentificarea trebuie să se facă rapid şi fără asistenţa unei persoane de specialitate, în situaţii dintre cele mai diverse. Este suficient să ne gândim doar la utilizarea amprentei pentru permiterea accesului la propriul telefon mobil, pentru a înţelege că folosirea amprentelor în scopul autentificării nu ar fi posibilă în absenţa unei tehnologii care să permită recunoaşterea aproape imediată a caracteristicilor biometrice. În afara avantajului rapidităţii, utilizarea tehnologiei prezintă şi avantajul acurateţei. Identificarea după amprente presupune, teoretic, găsirea identităţii între trăsăturile comparate, respectiv evidenţierea situaţiilor în care nu există identitate[6]. Pentru aceasta, trebuie comparate detalii de mare fineţe, iar această operaţiune se poate face în mod riguros şi rapid cu ajutorul tehnologiei.

În prezent, există un interes crescând pentru aspectele referitoare la utilizarea biometriei, în special deoarece oamenii observă avantajele pe care utilizarea caracteristicilor biometrice le poate avea. De asemenea, interesul este generat şi de alţi factori, precum scăderea preţului senzorilor şi îmbunătăţirea tehnologiei utilizate. În paralel, se constată o creştere a conştientizării la scară largă a necesităţii de a evidenţia punctele tari şi punctele slabe ale demersului de utilizare a tehnologiei pentru identificarea sau autentificarea cu ajutorul elementelor biometrice[7]. Avantajele utilizării biometriei prin intermediul tehnologiei sunt evidente, dar nu trebuie să pierdem din vedere faptul că o simplă eroare în funcţionarea tehnologiei ne poate face extrem de vulnerabili şi poate compromite siguranţa la care aspirăm tocmai prin utilizarea tehnologiei în analiza parametrilor biometrici.

Amprentele digitale reprezintă prima categorie de parametri biometrici pentru analiza cărora s-a folosit tehnologia computerizată. La începutul anilor ’60 ai secolului XX, crearea componentelor de hardware capabile să proceseze suficient de bine imaginea amprentelor a făcut posibilă analiza computerizată a amprentelor. În anii ’80 ai secolului XX, dezvoltarea tehnologiei calculatoarelor personale şi dezvoltarea scannerelor optice au permis utilizarea identificării prin amprente şi în alte domenii decât cel al investigaţiilor penale. Procentul mare de utilizare a amprentelor digitale pentru identificare şi autentificare este dat de faptul că metoda este relativ uşor de folosit, este relativ ieftină şi prezintă grad mare de acurateţe, atât în investigaţiile penale, cât şi în asigurarea securităţii în diferite activităţi cotidiene. În plus, metoda nu este invazivă[8].

[6] Vom vedea, mai jos, că prin utilizarea tehnologiei în analiza amprentelor este dificil de obținut concluzia identității, la modul absolut.

[7] A. Jain *et al.*, *Introduction to Biometrics, op. cit.*

[8] L. O'Gorman, *Fingerprint Verification*, în A. Jain, R. Bolle, S. Pankanti (editori), *Biometrics. Personal Identification in Networked Society*, Springer, Boston, MA, 1996, pp. 43-44, [Online] la https://doi.org/10.1007/0-306-47044-6_2, accesat 17.11.2021; T. Frater, *op. cit.*

2. Scurt istoric al utilizării amprentelor în identificarea persoanelor

În demersul nostru de a analiza provocările tehnologice care apar în utilizarea amprentelor digitale, considerăm că este important să realizăm un scurt istoric al utilizării amprentelor ca modalitate de identificare a persoanelor. Motivul este dat de faptul că, dintre toate caracteristicile biometrice, amprentele sunt cele care au fost utilizate pentru cea mai mare perioadă de timp, perioadă în care au demonstrat din plin utilitatea lor.

Dovezile arheologice sugerează că utilizarea amprentelor pentru a identifica o anumită persoană probabil se practica în anii 6000-7000 î.e.n., de exemplu de către asirieni, chinezi şi locuitorii oraşului Ierihon. Unele documente emise în societatea chineză erau sigilate cu un sigiliu din argilă, pe care emitentul îşi lăsa amprenta degetului mare. Pe unele cărămizi ale caselor din Ierihon au fost găsite perechi de amprente ale degetelor mari, aparţinând, probabil, celui care făcuse cărămizile. Unele piese din ceramică datând din acea perioadă conţin amprente. Desigur, în prezent nu putem şti exact care era scopul utilizării amprentelor[9]. Amprentele care, din modul în care au fost poziţionate, arată în mod clar faptul că au fost lăsate intenţionat, cum sunt cele de pe sigilii, ilustrează faptul că era recunoscută valoarea lor identificatoare. În ceea ce priveşte amprentele de pe obiectele create cu ajutorul mâinilor (cum sunt obiectele de ceramică sau cărămizile), acestea, în mod firesc, pot conţine amprente imprimate în timpul procesului de fabricaţie. Astfel de amprente „neintenţionate" pot apărea în locuri diverse şi de multe ori sunt amprente parţiale. Dacă, însă, amprentele de pe astfel de obiecte sunt totale şi se găsesc într-un anumit loc (de exemplu, pe partea bazală a vaselor din ceramică), ele pot ilustra faptul că s-a dorit în mod intenţionat lăsarea amprentei; în astfel de cazuri, amprenta poate fi interpretată ca o veritabilă „semnătură" a meşterului, deci având valoare identificatoare.

În 1686 Marcello Malpighi, profesor de anatomie la Universitatea din Bologna, realizează un studiu asupra desenului de pe degete şi observă faptul că acesta conţine creste, spirale şi curbe. În 1923, Joannes Evangelista Purkinje, profesor de anatomie la Universitatea Breslau, a publicat o lucrare în care descrie nouă tipuri de modele ale amprentelor[10]. Niciunul dintre cei doi oameni de ştiinţă menţionaţi nu a făcut vreo referire la valoarea identificatoare a amprentelor, dar observaţiile lor au încurajat cercetări ulterioare cu privire la amprente, inclusiv cu privire la posibilitatea de a utiliza amprentele pentru a identifica indivizii[11].

[9] R. Allen, P. Sankar, S. Prabhakar, *Fingerprint Identification Technology*, în J. Wayman, A. Jain, D. Maltoni, D. Maio (editori), *Biometric Systems*, Springer, London, 2005, p. 21, [Online] la https://doi.org/10.1007/1-84628-064-8_2, accesat 20.11.2021.

[10] J. Berry, D. A. Stoney, *History and Development of Fingerprinting*, în H. C. Lee, R. E. Gaensslen (editori), *Advances in Fingerprint Technology*, second edition, CRC Press, Boca Raton, 2001, p. 32.

[11] R. Allen *et al.*, *op. cit.*, p. 21.

Un moment de cotitură în privinţa utilizării amprentelor pentru identificare este reprezentat de descoperirea pe care a făcut-o Sir William Herschel. Acesta a fost un magistrat britanic, care, în timpul activităţii sale din Jungipoor, India, a utilizat, pentru identificarea persoanelor care erau părţi în diferite contracte, impresiunile întregii feţe palmare a mâinilor acestora. Se pare că metoda, utilizată începând cu 1856, a fost inspirată de superstiţiile populaţiei indigene. Analizând impresiunile mâinilor de la un număr mare de persoane, Herschel a realizat faptul că amprentele degetelor nu se repetau, desprinzând, astfel, concluzia că erau unice. Pentru a demonstra o altă caracteristică a amprentelor, fixitatea, Herschel şi-a monitorizat impresiunile propriilor degete, de-a lungul vieţii[12].

În anii '70 ai secolului XIX, Dr. Henry Faulds, un chirurg britanic ce activa în Japonia, a descoperit urme de degete pe ceramică veche şi, studiind aceste amprente, a conştientizat potenţialul lor în identificarea persoanelor. Faulds a dezvoltat o metodă de a clasifica modelele formate de dispunerea crestelor de degete. În 1880, Faulds a adus la cunoştinţa lui Charles Darwin descoperirile sale cu privire la amprente, iar acesta le-a trimis vărului său, Sir Francis Galton[13].

În 1892, în urma unui studiu sistematic privind valoarea identificatoare a amprentelor, Sir Francis Galton a publicat prima carte despre potenţialul individualizator al amprentelor, intitulată „Fingerprints". Galton a adus dovezi ştiinţifice la ceea ce Herschel şi Faulds bănuiseră, şi anume că amprentele sunt unice şi rămân neschimbate de-a lungul vieţii. Calculele lui Galton arătau că probabilitatea ca două amprente să fie identice este de 1 la 64 de miliarde. Sistemul de clasificare a amprentelor dezvoltat de Sir Francis Galton stă la baza sistemului care este folosit pe scară largă şi în prezent[14].

În 1892, Juan Vucetich, un ofiţer de poliţie din Argentina, a realizat prima identificare a autorului unei crime prin analiza amprentei digitale a acestuia, pe baza urmei unui deget murdar de sânge[15].

În 1897, Sir Edward Henry, un ofiţer de poliţie britanic din India, pe baza studiilor lui Sir Francis Galton, a realizat un sistem de clasificare a amprentelor care a fost adoptat de Scotland Yard în 1901 şi este în continuare folosit pe scară largă[16].

În prezentarea momentelor cruciale pentru conştientizarea valorii identificatoare a amprentelor nu putem să nu facem referire şi la activitatea lui Alphonse Bertillon, care a lucrat în cadrul poliţiei din Paris şi care, începând cu anul 1800, a dezvoltat sistemul de antropometrie. Sistemul antropometric presupunea măsurarea a diferiţi parametri corporali (dimensiunea craniului, înălţime, greutate, lungimea braţelor, a picioarelor, a degetului arătător etc.), despre care se credea că, luaţi în considerare în ansamblul lor, aveau potenţial ridicat de individualizare. Bertillon calculase că probabilitatea ca două persoane să prezinte aceleaşi dimensiuni la aceiaşi parametri era de 1 la 4 milioane. Acest sistem a fost

[12] *Ibidem.*
[13] *Idem*, p. 22.
[14] *Ibidem.*
[15] *Ibidem.*
[16] *Ibidem.*

folosit la clasificarea persoanelor condamnate şi la identificarea recidiviştilor. Totuşi, sistemul dezvoltat de Alphonse Bertillon s-a dovedit a nu fi atât de precis pe cât se credea. De exemplu, s-a descoperit că doi prizonieri, ambii numiţi William West, aveau aproape aceleaşi dimensiuni ale parametrilor antropometrici[17]. Situaţiile de acest gen, precum şi dificultatea de a folosi sistemul propus de Bertillon, a dus la scăderea treptată a gradului de utilizare a sistemului antropometric de către poliţie. În anul 1915, doar ţara natală a lui Bertillon, Franţa, mai utiliza acest sistem, dar, în cele din urmă, şi Franţa a renunţat la el. Pentru a înlocui sistemul antropometric, au fost căutate metode cu o mai mare acurateţe şi mai uşor de folosit, ceea ce a creat condiţiile pentru folosirea la scară din ce în ce mai mare a sistemului de identificare bazat pe amprente[18]. Oricum, trebuie menţionat faptul că Alphonse Bertillon a adus o contribuţie importantă şi în ceea ce priveşte utilizarea amprentelor, de exemplu observaţia sa că 12-15 puncte coincidente sunt suficiente pentru a desprinde concluzia identităţii[19].

3. Tipuri de verificare a amprentelor prin utilizarea tehnologiei

Identificarea cu ajutorul amprentelor prin utilizarea tehnologiei presupune desfăşurarea anterioară a unei operaţiuni de verificare. Această verificare prezintă o serie de particularităţi, în funcţie de scopul pentru care este utilizată amprenta[20].

Verificarea efectuată cu scopul de a permite unei persoane accesul la utilizarea unui bun sau la o anumită facilitate se numeşte potrivire unu-la-unu. În acest caz, verificarea presupune compararea unei amprente cu o amprentă care este deja înregistrată în sistem. În vederea verificării, o persoană trebuie, mai întâi, să-şi înregistreze amprenta în sistemul care este utilizat. Imaginea acelei amprente înregistrate este stocată în sistem, în format comprimat, iar apoi amprenta utilizatorului este comparată cu acea imagine[21].

Verificarea efectuată cu scopul identificării criminalistice se numeşte unu-la-mai-multe. În acest caz, imaginea unei amprente provenind de la o persoană necunoscută este comparată cu imaginile dintr-o bază de date ale amprentelor aparţinând unor persoane cu identitate cunoscută[22].

Există şi un al treilea tip, informal, de verificare, numit unu-la-câteva, care se aplică în situaţia în care un sistem de acces pe bază de amprentă este utilizat de

[17] *Idem*, p. 21.

[18] R. B. Fosdick, *Passing of the Bertillon System of Identification*, în Journal of Criminal Law and Criminology, Vol. 6, Nr. 3/1915, pp. 363-369, [Online] la https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1374&context=jclc, accesat 22.11.2021,

[19] A. Bertillon, *Notes et observations médico-légales. Les empreintes digitales*, în Archives d'anthropologie criminelle de médecine légale et de psychologie normale et pathologique, Vol. 27/1912, p. 52, [Online] la https://criminocorpus.org/ en/ref/114/20706/, accesat 22.11.2021,.

[20] L. O'Gorman, *Fingerprint Verification*, *op. cit.*, p. 45.

[21] *Ibidem.*

[22] *Ibidem.*

un număr redus de persoane, de exemplu atunci când membrii unei familii folosesc un sistem bazat pe amprente pentru a intra în casă[23].

4. Procedura identificării prin analiza amprentei, cu ajutorul tehnologiei

Primul pas în realizarea identificării cu ajutorul amprentelor, prin utilizarea tehnologiei, este realizarea unei imagini a amprentei. Ulterior, are loc procesarea imaginii, al cărei scop este de a se obţine cea mai bună imagine posibilă, pentru a avea un rezultat corect după verificare[24].

În esenţă, procedura de identificare cu ajutorul amprentei trebuie să parcurgă următoarele etape: reducerea neclarităţii şi îmbunătăţirea imaginii, detectarea (sau *extragerea*) caracteristicilor şi verificarea potrivirii. În continuare, vom prezenta detalii privind aceste etape.

4.1. Reducerea neclarităţii şi îmbunătăţirea imaginii

Imaginea unei amprente este, de regulă, neclară, în special datorită faptului că degetele sunt de cele mai multe ori acoperite cu diferite substanţe, precum murdărie, transpiraţie, sebum etc. Acest pas urmăreşte, în primul rând, sporirea contrastului dintre creste şi şanţuri. Pentru obţinerea acestui rezultat, se utilizează filtrele adaptive potrivite şi pragurile adaptive[25].

O trăsătură a desenului papilar care se dovedeşte a fi utilă în procesarea imaginii amprentei este aşa-numita „redundanţă" a crestelor paralele, care poate fi folosită pentru a crea un filtru adaptiv potrivit. Acest filtru se aplică fiecărui pixel al imaginii. Pe baza orientării locale a crestelor în jurul fiecărui pixel, se aplică filtrul adaptiv pentru a evidenţia crestele orientate în aceeaşi direcţie, în acelaşi timp estompând tot ceea ce are o orientare diferită. De exemplu, particulele de murdărie care „îmbâcsesc" amprenta pot uni două creste învecinate, dar aceste particule, fiind perpendiculare pe aceste creste, au o direcţie diferită, deci vor fi identificate drept elemente care nu fac parte din imaginea amprentei propriu-zise. Identificarea se face cu ajutorul filtrului adaptiv, care are în vedere cursul firesc al crestelor[26].

Ulterior, are loc binarizarea, adică separarea crestelor de fundal. Acest proces facilitează desfăşurarea paşilor următori de analiză a amprentei. Practic, în timpul operaţiunii de binarizare, are loc transformarea unei imagini care, iniţial, este în tonuri de gri, într-o imagine binară. Operaţiunea de binarizare este destul de dificilă, deoarece nu toate imaginile amprentelor au aceleaşi specificaţii privind contrastul, ceea ce înseamnă că nu se poate alege acelaşi prag de intensitate. Mai mult, contrastul poate varia chiar în cadrul aceleiaşi imagini, de exemplu dacă presiunea cu care a fost creată urma de deget a fost mai mare în mijlocul desenului

[23] *Ibidem.*
[24] *Ibidem.*
[25] *Idem*, p. 47.
[26] *Idem*, pp. 47-48.

papilar. Pentru a depăşi această dificultate, este utilizat un procedeu numit prag adaptiv local[27].

În continuare, are loc procesul de subţiere a crestelor, care reduce grosimea crestelor, chiar până la 1 pixel. Această operaţiune uşurează detectarea unor detalii ale amprentei, precum sfârşitul de creastă şi bifurcaţia[28].

Procedura de reducere a neclarităţii şi de îmbunătăţire a imaginii necesită un interval de timp destul de îndelungat. Din acest motiv, unele sisteme de analiză a amprentelor sunt create astfel încât să se desfăşoare cât mai repede această etapă, dar o astfel de abordare poate compromite rezultatul final. Desfăşurarea tuturor operaţiunilor subsecvente depinde de calitatea imaginii, aşa cum este ea obţinută în această etapă. Din acest motiv, se recomandă ca sistemele de analiză a amprentelor să nu sacrifice calitatea rezultatului final, de dragul desfăşurării cât mai rapide a procesului de identificare[29].

4.2. Detectarea caracteristicilor

Detectarea caracteristicilor este relativ uşor de realizat, după ce imaginea a fost procesată în etapa anterioară. De regulă, chiar dacă mai există erori, în sensul că apar detalii „false", ele pot fi detectate prin utilizarea pragurilor determinate empiric. De exemplu, dacă se constată două capetele de creastă care sunt foarte apropiate unul de celălalt, se consideră că acestea fac parte din aceeaşi creastă, iar discontinuitatea a apărut, probabil, datorită unei cicatrici sau datorită faptului că degetul era uscat când a fost creată amprenta. În urma procedeului de detectare a caracteristicilor se obţine *minutia template*, adică un model al detaliilor şi al locului ocupat de acestea. De regulă, în această etapă sunt detectate 10 până la 100 de detalii, în funcţie de diferiţi factori, de exemplu în funcţie de calitatea imaginii iniţiale[30].

4.3. Verificarea potrivirii

În această etapă are loc compararea amprentei analizate cu o amprentă care este deja înregistrată în sistem. În principiu, verificarea presupune compararea vecinătăţilor detaliilor apropiate, căutându-se indicii de similaritate[31]. Dacă, în urma comparării, apar doar foarte mici diferenţe, atunci concluzia va fi cea de *potrivire* a vecinătăţilor. Această procedură de comparare se face exhaustiv pentru

[27] *Idem*, p. 48.
[28] *Ibidem.*
[29] *Ibidem.*
[30] *Idem*, p. 50.
[31] Precizăm că am folosit intenționat cuvântul „similaritate" și nu cuvântul „identitate". Aceasta, deoarece va exista rar o potrivire exactă a vecinătăților, din două motive: neclaritatea amprentei, care provine din faptul că degetul este, de regulă, îmbâcsit cu diverse substanțe; caracteristicile pielii, care este un țesut elastic, ceea ce înseamnă că vor exista frecvent mici variații în aspectul și dispunerea detaliilor. A se vedea L. O'Gorman, *Fingerprint Verification*, *op. cit.*, p. 50.

toate combinaţiile de vecinătăţi şi, dacă există suficiente similarităţi, atunci concluzia privind întreaga amprentă va fi de potrivire[32].

În urma operaţiunii de verificare se formulează o concluzie privind gradul de potrivire, concluzie care, de regulă, se exprimă sub forma unui număr de la 0 la 1 sau de la 10 la 100. Rezultatul obţinut se compară cu un prag predeterminat. Dacă rezultatul este mai mare decât pragul, concluzia generală va fi de potrivire, iar dacă rezultatul este mai mic decât pragul, concluzia va fi de nepotrivire. Dacă pragul este stabilit la o valoare mai mare, atunci va creşte probabilitatea de a obţine potriviri corecte, dar va exista un risc mai mare de a obţine respingeri false. Dacă pragul este stabilit la o valoare mai mică, atunci va scădea riscul de a obţine respingeri false, dar creşte riscul de potriviri false. În cazul sistemelor de verificare a amprentelor pentru uz comercial, valoarea pragului va fi stabilită, de regulă, de către structura care pune sistemul la dispoziţia utilizatorilor[33].

5. Particularităţi ale utilizării tehnologiei pentru analiza amprentelor în Criminalistică

Pentru analiza amprentelor în cadrul unei investigaţii criminalistice, de multe ori trebuie realizată o comparare a unei amprente cu amprentele existente într-o bază de date, care poate conţine câteva zeci de milioane de imagini de amprente. Compararea unei amprente ridicate de la faţa locului cu absolut toate amprentele dintr-o bază de date ar necesita alocarea unui interval foarte mare de timp, ceea ce ar încetini desfăşurarea anchetei. Din acest motiv, utilizarea tehnologiei pentru analiza amprentelor în scop criminalistic presupune, de regulă, două etape. În prima etapă, se stabileşte categoria din care face parte amprenta care urmează a fi analizată. În a doua etapă, se compară detaliile de pe amprenta analizată şi cele de pe amprentele din baza de date care fac parte din aceeaşi categorie cu amprenta analizată[34].

6. Concluzii privind provocările tehnologice în crearea standardelor pentru analiza amprentelor digitale

Aşa cum am văzut în cele expuse mai sus, tehnologia este absolut necesară în demersul de utilizare a amprentelor, atât în scopul identificării în cadrul investigaţiilor penale, cât şi în scopul autentificării pentru permiterea accesului, în diverse situaţii. În acelaşi timp, aspectele prezentate evidenţiază complexitatea tehnologiei utilizate în analiza amprentelor şi vulnerabilităţile care pot apărea. Am arătat că, în urma utilizării tehnologiei pentru identificarea unei persoane cu ajutorul amprentei, maximul care se poate obţine nu este o certitudine a identităţii, ci doar o *potrivire optimă*, bazată pe o similaritate foarte mare. Am văzut că, pentru

[32] L. O'Gorman, *Fingerprint Verification*, *op. cit.*, pp. 50-51.
[33] *Idem*, p. 51.
[34] *Ibidem.*

obţinerea unui răspuns, trebuie setat de către factorul uman un anumit prag, a cărui valoare poate influenţa semnificativ rezultatul.

În acest context, apare ca necesară standardizarea tehnologiei de utilizare a amprentelor, mai ales ţinând cont de faptul că necesitatea verificării amprentelor poate apărea nu doar punctual, într-o situaţie dată, ci în situaţii variate, pe plan naţional şi internaţional.

De exemplu, schimbul de informaţii privind amprentele în cadrul cooperării penale internaţionale trebuie să se bazeze pe o compatibilitate foarte bună a sistemelor tehnologice folosite pentru transmiterea, respectiv receptarea informaţiei. Dacă algoritmii de criptare a informaţiei transmise nu se potrivesc cu algoritmii de decriptare pe care îi deţine receptorul, atunci, practic, nu se poate face transferul de informaţii. Dacă imaginea iniţială a amprentei încărcată în sistem nu este de bună calitate, de asemenea, se poate compromite rezultatul, deci ar fi nevoie şi de un standard al imaginilor încărcate.

Un alt exemplu poate fi dat din domeniul autorizării accesului la utilizarea unui automat bancar (ATM) prin analiza amprentei[35]. În lipsa unui standard, în funcţie de tehnologia utilizată şi în funcţie de pragul de potrivire ales, unele bancomate ar putea să permită rapid accesul, altele ar putea avea o rată mare de falsă respingere, această din urmă situaţie ducând la nemulţumire în rândul utilizatorilor.

Aspectele prezentate ilustrează faptul că este necesar a se crea noi standarde, pe măsură ce creşte gradul de utilizare a tehnologiei pentru analiza amprentelor. Însă este dificil de impus standarde în acest domeniu, cu atât mai mult cu cât unele standarde ar trebui adoptate la nivel internaţional. În crearea standardelor, particularităţile de ordin tehnologic joacă un rol foarte important. De asemenea, scopul pentru care este utilizată o anumită tehnologie de recunoaştere a amprentei are un rol major. În acest context, credem că trebuie acordată atenţie armonizării tuturor elementelor în discuţie, astfel încât identificarea persoanelor prin intermediul amprentelor să aibă o rată cât mai mare de reuşită şi să se elimine neclarităţile care, încă, mai există în acest domeniu.

Referinţe

Allen R., Sankar P., Prabhakar S., *Fingerprint Identification Technology*, în Wayman J., Jain A., Maltoni D., Maio D. (editori), *Biometric Systems*, Springer, London, 2005, pp. 22-61, https://doi.org/10.1007/1-84628-064-8_2

Berry J., Stoney D. A., *History and Development of Fingerprinting*, în Lee H. C., Gaensslen R. E. (editori), *Advances in Fingerprint Technology*, second edition, CRC Press, Boca Raton, 2001, pp. 14-53

Bertillon A., *Notes et observations médico-légales. Les empreintes digitales*, în Archives d'anthropologie criminelle de médecine légale et de psychologie normale et pathologique, Vol. 27/1912, pp. 36-52

[35] Pentru detalii, a se vedea T. Sangeetha, M. Kumaraguru, S. Akshay, M. Kanishka, *Biometric Based Fingerprint Verification System for ATM Machines*, în Journal of Physics: Conference Series, 1916, 2021, 012033, [Online] la https://doi.org/10.1088/1742-6596/1916/1/012033, accesat 29.11.2021.

Fosdick R. B., *Passing of the Bertillon System of Identification*, în Journal of Criminal Law and Criminology, Vol. 6, Nr. 3/1915, pp. 363-369

Frater T., *Standards for Fingerprint Indentification*, [Online]

Jain A., Bolle R., Pankanti S., *Introduction to Biometrics*, în Jain A., Bolle R., Pankanti S. (editori), *Biometrics*, Springer, Boston, MA, 1996, pp. 1-41, https://doi.org/10.1007/0-306-47044-6_1

Jain A., Pankanti S, *Automated Fingerprint Identification and Imaging Systems*, în Lee H. C., Gaensslen R. E. (editori), *Advances in Fingerprint Technology*, second edition, CRC Press, Boca Raton, 2001, pp. 285-336

O'Gorman L., *An overview of fingerprint verification technologies*, în Information Security Technical Report, Vol. 3, Nr. 1/1998, pp. 21-32, https://doi.org/10.1016/S1363-4127(98)80015-0

O'Gorman L., *Fingerprint Verification*, în Jain A., Bolle R., Pankanti S. (editori), *Biometrics. Personal Identification in Networked Society*, Springer, Boston, MA, 1996, pp. 43-64, https://doi.org/10.1007/0-306-47044-6_2

Sangeetha T., Kumaraguru M., Akshay S., Kanishka M., *Biometric Based Fingerprint Verification System for ATM Machines*, în Journal of Physics: Conference Series 1916, 2021, 012033, https://doi.org/10.1088/1742-6596/1916/1/012033

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-21

Directiva NIS: elaborarea unei reglementări-cadru privind securitatea informaţiilor din UE

The NIS Directive: Developing the EU Cybersecurity Regulatory Framework

Ştefan Răzvan Tataru[1]

Rezumat: Ultimele decenii sunt caracterizate prin digitalizare şi inovare tehnologică, evoluţie care a determinat atât eficientizarea activităţilor economice dar şi riscuri asupra securităţii informaţiilor de afaceri şi a datelor cu caracter personal. Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice – Directiva NIS – vizează protejarea infrastructurilor critice şi digitale pentru asigurarea funcţionării sistemelor considerate esenţiale pentru populaţie, stabilind în sarcina operatorilor de servicii esenţiale şi a furnizorilor de servicii digitale obligaţia de a implementa măsuri minime de protecţie corelate cu riscurile la securitatea sistemelor informatice. În prezentul studiu ne propunem să analizăm modul în care Directiva NIS impactează afacerile şi, totodată, să evaluăm interacţiunea prevederilor acesteia cu cele ale Regulamentului UE 2016/679 – Regulamentul general privind protecţia datelor cu caracter personal (GDPR).

Cuvinte-cheie: Directiva NIS; NIS; GDPR; protecţia datelor; securitatea informaţiei; securitate cibernetică

Abstract: The last decades are characterized by digitalization and technological innovation, an evolution that has determined both the efficiency of economic activities and risks on the security of business information and personal data. Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems – the NIS Directive – aims to protect critical and digital infrastructures to ensure the functioning of systems considered essential for the population, laying down essential service operators and digital service providers the obligation to implement minimum protection measures related to the risks to the security of information systems. In this study we aim to analyse how the NIS Directive impacts business and, at the same time, to evaluate the interaction of its provisions with those of EU Regulation 2016/679 – General Regulation on the protection of personal data (GDPR).

Keywords: NIS Directive; NIS; GDPR; data protection; information security; cybersecurity

[1] Doctor în drept, cadru didactic asociat, Facultatea de Economie şi Administrarea Afacerilor, Universitatea „Alexandru Ioan Cuza” din Iaşi, e-mail: razvantataru@gmail.com, Orcid ID 0000-0002-1746-9636.

1. Introducere

Ultimele decenii sunt caracterizate prin digitalizare şi inovare tehnologică, evoluţie care a determinat atât eficientizarea activităţilor economice dar şi riscuri asupra securităţii informaţiilor de afaceri şi a datelor cu caracter personal. Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice[2] – Directiva NIS - vizează protejarea infrastructurilor critice şi digitale pentru asigurarea funcţionării sistemelor considerate esenţiale pentru populaţie, stabilind în sarcina operatorilor de servicii esenţiale şi a furnizorilor de servicii digitale obligaţia de a implementa măsuri minime de protecţie corelate cu riscurile la securitatea sistemelor informatice. Dezideratul Uniunii Europene de a implementa o strategie de securitate cibernetică comună şi eficientă la nivelul statelor membre a devenit o necesitate stringentă în contextul celei de-a patra revoluţii industriale. Astfel, în contextul în care activităţile productive au fost digitalizate complet, utilizarea inteligenţei artificiale şi a tehnologiilor cognitive reprezintă o condiţie de supravieţuire a întreprinderilor într-o piaţa internaţională competitivă, dispozitivele *Internet of things (IoT)*[3] sunt uşor accesibile şi de implementat, iar Internetul reprezintă un instrument disponibil pentru eficientizarea tuturor activităţilor[4], garanţia unor măsuri de securitate asupra informaţiilor şi sistemelor informatice care permit şi, totodată, condiţionează desfăşurarea în condiţii normale a activităţilor reprezintă o necesitate absolută. Incidentele de securitate cibernetică sunt însoţite adeseori de urmări grave care afectează securitatea datelor şi a sistemelor informatice, determinând totodată pierderi financiare şi şi care determină, în termeni de securitate, de pierderi economice şi financiare şi de afectare a imaginii organizaţiei[5].

În lipsa implementării unor măsuri adecvate de securitate a reţelelor şi sistemelor informatice, atacurile cibernetice reprezintă o ameninţare gravă care poate cauza întreruperi ale serviciilor IT şi ale infrastructurilor critice, determinând deopotrivă blocaje în desfăşurarea activităţilor economice, pierderi financiare substanţiale, subminarea încrederii utilizatorilor şi pagube majore economiei

[2] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, publicată în JO L 194 din data de 19.07.2016.

[3] Pentru detalii privind tehnologiile *Artificial Intelligence (AI)* sau *Internet-of-Things (IoT)* a se vedea C.T. Ungureanu, *Drept internațional privat european în raportul de comerț internațional*, Editura Hamangiu, 2021, p. 354 și urm.

[4] C.T. Ungureanu, *Implicațiile Internetului în viața juridică*, Analele Științifice ale Universitații „Alexandru Ioan Cuza" Iași, Tomul LXIII, Științe Juridice, 2017, nr. II, pp. 1-2; Ș.R. Tataru, *Internet Cookies - fișierele cu răvaș juridic*, în Analele Științifice ale Universităţii „Alexandru Ioan Cuza" din Iași, Tomul LXVI, Supliment, Științe Juridice, 2020, p. 33

[5] Serviciul Român de Informații, *Ghid de bune practice pentru securitatea cibernetică*, [Online] la https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica. pdf, accesat 11.11.2021.

Uniunii[6]. Directiva NIS abordează această nevoie prin stabilirea măsurilor necesare „obţinerii unui nivel comun ridicat de securitate a reţelelor şi a sistemelor de informaţii în cadrul Uniunii, astfel încât să îmbunătăţească funcţionarea pieţei interne”[7].

2. „Reglementările” NIS

Uniunea Europeană nu abordează problematica securităţii cibernetice pentru prima dată în anul 2016, prin intermediul Directivei NIS, preocuparea pentru crearea unui mediu online securizat fiind manifestată încă din anul 2014 când a fost fondată ENISA (Agenţia Uniunii Europene pentru Securitatea Reţelelor şi Informaţiilor)[8].

Directiva (UE) 2016/1148 a Parlamentului European şi a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune stabileşte cadrul juridic şi instituţional, măsurile şi mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice şi a stimulării cooperării în domeniu[9]. Directiva (UE) 2016/1148, cunoscută sub denumirea de Directiva NIS (*Network and Information Security*) reprezintă prima reglementare complexă la nivel comunitar privind securitatea cibernetică şi totodată, una dintre cele mai importante componente ale strategiei Uniunii Europene în acest domeniu[10]. Prevederile Directivei NIS permit statelor membre să stabilească prin intermediul legislaţiei naţionale standarde care să asigure un nivel mai ridicat de securitate. În acest sens, statele membre pot extinde obligaţiile de securitate şi notificare prevăzute pentru operatorii de servicii esenţiale şi la entităţi aparţinând altor sectoare şi subsectoare nu numai la cele enumerate în anexa la Directiva NIS.

În România, Directiva nr. 2016/1148 a fost transpusă în legislaţia naţională prin intermediul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, publicată în Monitorul Oficial, Partea I nr. 21 din 9 ianuarie 2019.

---

[6] D. Markopoulou, V. Papakonstantinou, P. de Hert, *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, Computer Law & Security Review 35 (2019) 105336, p. 1.

[7] Conform art. 1 alin. (1) din Directiva (UE) 2016/1148.

[8] N. Saqib, V. Germanos, W. Zeng , L. Maglaras, *Mapping of the Security Requirements of GDPR and NIS*, în Preprints, iunie 2020, p. 4, [Online] la https://www.preprints.org/manuscript/202006.0193/v1, accesat 11.11.2021; D. Markopoulou, V. Papakonstantinou, P. de Hert, *op. cit.*, p. 2.

[9] A se vedea şi art. 1 din Legea nr. 362/2018.

[10] A se vedea website-ul Agenţiei Uniunii Europene pentru Securitatea Reţelelor şi Informaţiilor (ENISA), secţiunea Directiva NIS, [Online] la https://www.enisa.europa.eu/topics/nis-directive, accesat 11.11.2021.

2.1. Operatori de Servicii Esenţiale vs. Furnizori de Servicii Digitale

Spre deosebire de Regulamentul GDPR care are un domeniu de aplicare material vast, determinând obligaţii pentru toţi operatorii de date cu caracter personal, Directiva NIS vizează doar instituţii, autorităţi sau societăţi care au calitatea de Operatori de Servicii Esenţiale (OSE) sau de Furnizori de Servicii Digitale (FSD)[11].

Conform art. 4 pct. 4 din Directivă, operatorul de servicii esenţiale (OSE) desemnează o entitate publică sau privată care activează într-unul dintre sectoarele specifice menţionate în Anexa nr. 2 şi care îndeplineşte cumulativ următoarele condiţii[12]: a) furnizează un serviciu esenţial pentru susţinerea activităţilor societale şi/sau economice de cea mai mare importanţă; b) furnizarea serviciului respectiv depinde de reţea şi de sistemele informatice; şi c) un incident ar avea efecte perturbatoare semnificative asupra furnizării serviciului. Anexa nr. 2 a Directivei prevede şapte sectoare de activitate economică astfel: Energie, Transport, Sectorul bancar, Infrastructuri ale pieţei financiare, Sectorul sănătăţii, Furnizarea şi distribuirea de apă potabilă şi Infrastructură digitală.

În prezent, se află în dezbatere propunerea[13] de Directivă NIS 2.0 care aduce o serie de modificări majore, dintre care menţionăm extinderea sectoarelor reglementate pentru entităţile esenţiale, de la şapte la zece sectoare. Astfel, Directiva NIS 2.0 lărgeşte sfera operatorilor de servicii esenţiale prin adăugarea următoarelor sectoare de activitate: Colectarea, eliminarea sau tratarea apei uzate/reziduale, Administraţia publică şi Spaţiul cosmic[14].

Furnizorii de servicii digitale (FSD) reprezintă orice persoană juridică care furnizează un serviciu digital[15], respectiv: pieţele online, motoarele de căutare web şi serviciile de cloud-computing. Reglementarea naţională – Legea nr. 362/2018,

[11] Pentru detalii a se vedea M.D. Cole, S. Schmitz, *The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape,* în University of Luxembourg Law Working Paper No. 2019-017, December 31, 2019, [Online] la http://dx.doi.org/10.2139/ssrn.3512093, accesat 11.11.2021.

[12] A se vedea art. 5 alin. (2) din Directiva NIS.

[13] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final, [Online] la https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN, accesat 11.11.2021.

[14] A se vedea și website-ul Directoratului Național de Securitate Cibernetică, [Online] la https://dnsc.ro/citeste/includerea-administratiei-publice-intre-sectoarele-nis-2, accesat 11.11.2021.

[15] Conform art. 4 alin. (5) din Directiva NIS, *„serviciu digital"* înseamnă un serviciu în sensul articolului 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului (17) care este de un tip enumerat în anexa III; Astfel, actul normative la care face trimitere Directiva NIS definește serviciul digital drept *„orice serviciu al societății informaționale, adică orice serviciu prestat în mod normal în schimbul unei remunerații, la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciului".*

defineşte conceptul de „serviciu digital”[16] prin trimitere la art. 4 alin. (1) pct. 2 din Hotărârea Guvernului nr. 1.016/2004 privind măsurile pentru organizarea şi realizarea schimbului de informaţii în domeniul standardelor şi reglementărilor tehnice, precum şi al regulilor referitoare la serviciile societăţii informaţionale între România şi statele membre ale Uniunii Europene, drept acel *„serviciu [...] care se încadrează într-una din categoriile: 1. piață online*[17]*; 2. motor de căutare online*[18]*; 3. serviciu de cloud computing*[19]*”*. Definirea limitativă a furnizorilor de servicii digitale prin raportare doar la cele trei tipuri de servicii este justificată prin numărul tot mai mare de persoane care depind fundamental de ele pentru furnizarea propriilor servicii.

2.2. Obligaţii legale conform NIS

Directiva NIS defineşte în cadrul articolelor 14-18 cerinţele de securitate şi notificarea incidentelor pentru operatorii de servicii esenţiale şi, respectiv, furnizorii de servicii digitale. În cadrul reglementărilor naţionale, obligaţiile impuse operatorilor de servicii esenţiale şi furnizorilor de servicii digitale se regăsesc în cadrul art. 10-12 din Legea nr. 362/2018.

În conformitate cu art. 14 alin. (1) din Directiva NIS, statele membre sunt obligate să se asigure că operatorii de servicii esenţiale iau măsuri corespunzătoare, tehnice şi organizatorice, pentru a gestiona riscurile prezentate pentru securitatea reţelei şi a sistemelor informatice pe care le utilizează. În conformitate cu art. 14 alin. (2), măsurile adecvate trebuie să prevină şi să reducă la minimum impactul incidentelor care afectează securitatea sistemelor lor, dezideratul urmărit fiind asigurarea continuităţii serviciilor esenţiale.

Din analiza prevederilor Directivei NIS şi a Legii nr. 362/2018 putem observa faptul că obligaţiile ce revin operatorilor de servicii esenţiale pot fi clasificate în a) obligaţii de a asigura implementarea unor măsuri minime de securitate şi b) obligaţii de notificare a incidentelor de securitate.

---

[16] A se vedea art. 3 lit. o) din Legea nr. 362/2018.

[17] Directiva NIS definește „piața online” drept *„un serviciu digital care permite consumatorilor și/sau comercianților [...], să încheie online vânzări sau contracte de servicii cu comercianți fie pe site-ul internet al pieței online, fie pe site-ul internet al unui comerciant care utilizează servicii informatice furnizate de piața online”* – a se vedea art. 4 pct. 17.

[18] Motorul de căutare online este *„un serviciu digital care permite utilizatorilor să caute, în principiu, în toate site-urile internet sau site-urile internet într-o anumită limbă pe baza unei interogații privind orice subiect sub forma unui cuvânt, a unei fraze sau a unei alte informații-cheie și care revine cu linkuri în care se pot găsi informații legate de conținutul căutat”* – a se vedea art. 4 pct. 18.

[19] Conform art. 4 pct. 19 din Directiva NIS, „serviciu de cloud-computing” înseamnă un serviciu digital care permite accesul la un bazin redimensionabil și elastic de resurse informatice care pot fi puse în comun. Pentru detalii privind conceptul de cloud-computing a se vedea C.T. Ungureanu, *Contractul Cloud Computing în comerţul internaţional*, Revista Moldovenească de Drept Internațional și Relații Internaționale Nr. 3 (37), 2015, pp. 26-27.

2.2.1. Obligaţii pentru Operatorii de servicii esenţiale

Operatorii de servicii esenţiale, spre deosebire de furnizorii de servicii digitale, se identifică şi se înscriu în Registrul operatorilor de servicii esenţiale[20]. Astfel, conform art. 8 din Legea nr. 362/2018, entităţile care îndeplinesc condiţiile şi criteriile stabilite pentru a se califica drept operator de servicii esenţiale au obligaţia de a notifica CERT-RO[21] (Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică) în vederea înscrierii în Registrul operatorilor de servicii esenţiale în termen de 30 de zile de la data îndepliniri acestora.

Dintre principalele obligaţiile ce revin operatorilor de servicii esenţiale în conformitate cu prevederile art. 10 din Legea nr. 362/2018, amintim: *„a) implementează măsurile tehnice şi organizatorice adecvate şi proporţionale pentru îndeplinirea cerinţelor minime de securitate [...]; b) implementează măsuri adecvate pentru a preveni şi minimiza impactul incidentelor care afectează securitatea reţelelor şi a sistemelor informatice utilizate pentru furnizarea acestor servicii esenţiale, cu scopul de a asigura continuitatea serviciilor respective [...]; c) notifică de îndată CERT-RO în calitate de CSIRT naţional incidentele care au un impact semnificativ asupra continuităţii serviciilor esenţiale [...]; d) pun la dispoziţia CERT-RO informaţii care să permită stabilirea impactului transfrontalier al incidentului [...];h) se interconectează [...] la serviciul de alertare şi cooperare al CERT-RO, asigură monitorizarea permanentă a alertelor şi solicitărilor primite prin acest serviciu ori prin celelalte modalităţi de contact şi ia în cel mai scurt timp măsurile adecvate de răspuns la nivelul reţelelor şi sistemelor informatice proprii; i) asigură de îndată răspunsul la incidentele survenite, restabilesc în cel mai scurt timp funcţionarea serviciului la parametrii dinaintea incidentului şi realizează auditul de securitate [...]”.*

Conform celor anterior precizate, cerinţele de securitate care trebuie adoptate de operatorii de servicii esenţiale sunt însoţite de obligaţia de a notifica autorităţile competente cu privire la orice incident care are un impact asupra continuităţii serviciilor esenţiale pe care le oferă un operator. În conformitate cu art. 14 alin. (3) din Directiva NIS, statele membre trebuie să se asigure că operatorii de servicii esenţiale notifică „*orice incident care are un impact semnificativ asupra continuităţii serviciilor esenţiale pe care le furnizează*”. În stabilirea impactului unui incident de securitate, operatorul de servicii esenţiale va avea în vedere prevederile art. 14 alin. (4) din Directivă care furnizează o listă a parametrilor care trebuie luaţi în considerare, şi anume: numărul de utilizatori afectaţi, durata incidentului şi răspândirea geografică în raport cu zona afectată de incident. Mai mult decât atât,

[20] Conform art. 5 din Legea nr. 362/2018. A se vedea şi N. Saqib, V. Germanos, W. Zeng, L. Maglaras, *op. cit.,* p. 7.

[21] În România, Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică CERT-RO reprezintă autoritatea competentă la nivel naţional sau echipa de răspuns la incidente de securitate informatică (CSIRT). Începând din 24 septembrie 2021, CERT-RO a fost desfiinţat iar atribuţiile acestuia au fost preluate de către Directoratul Naţional de Securitate Cibernetică (DNSC). Pe parcursul prezentului articol au fost utilizate ambele denumiri, respectiv CERT-RO şi DNSC, în funcţie de actul normativ indicat, ambele desemnând aceeaşi entitate – CSIRT naţional din România.

conform art. 10 alin. (3) din Legea nr. 362/2018, operatorii de servicii esenţiale trebuie să notifice de îndată echipa naţională de intervenţie în caz de incidente de securitate informatică (*Computer Security Incident Response Team – CSIRT*[22]) şi în situaţia în care afectarea serviciilor esenţiale se datorează unor incidente care afectează un furnizor de servicii digitale de care depinde furnizarea serviciilor esenţiale.

Cerinţele minime de securitate sunt stabilite de către CERT-RO prin normele tehnice, operatorii de servicii esenţiale având obligaţia de a le respecta în vederea asigurării unui nivel comun de securitate a reţelelor şi sistemelor informatice. *„Normele tehnice aplicabile operatorilor de servicii esenţiale se stabilesc în baza cel puţin a următoarelor categorii de activităţi de asigurare a securităţii reţelelor şi sistemelor informatice: a) managementul drepturilor de acces; b) conştientizarea şi instruirea utilizatorilor; c) jurnalizarea şi asigurarea trasabilităţii activităţilor în cadrul reţelelor şi sistemelor informatice; d) testarea şi evaluarea securităţii reţelelor şi sistemelor informatice; e) managementul configuraţiilor reţelelor şi sistemelor informatice; f) asigurarea disponibilităţii serviciului esenţial şi a funcţionării reţelelor şi sistemelor informatice; g) managementul continuităţii funcţionării serviciului esenţial; h) managementul identificării şi autentificării utilizatorilor; i) răspunsul la incidente; j) mentenanţa reţelelor şi sistemelor informatice; k) managementul suporturilor de memorie externă; l) asigurarea protecţiei fizice a reţelelor şi sistemelor informatice; m) realizarea planurilor de securitate; n) asigurarea securităţii personalului; o) analizarea şi evaluarea riscurilor; p) asigurarea protecţiei produselor şi serviciilor aferente reţelelor şi sistemelor informatice; q) managementul vulnerabilităţilor şi alertelor de securitate”*[23].

Conform prevederilor art. 5 alin (5) în implementarea măsurilor de securitate, *„operatorii de servicii esenţiale: a) identifică reţelele şi sistemele informatice care susţin furnizarea de servicii esenţiale; b) elaborează şi implementează politici şi planuri proprii de securitate a reţelelor şi sistemelor informatice; c) asigură managementul incidentelor care afectează securitatea reţelelor şi sistemelor informatice; d) previn accesul neautorizat la reţelele şi sistemele informatice; e) previn diseminarea datelor deţinute la nivelul reţelelor şi sistemelor informatice către alte persoane decât cele autorizate să cunoască conţinutul acestora; f) implementează un sistem de management al riscului; g) implementează planuri de acţiune pe niveluri de alertă de securitate a reţelelor şi sistemelor informatice; h) asigură continuitatea serviciilor”.*

2.2.2. Obligaţii pentru Furnizorii de servicii digitale

Furnizorii de servicii digitale, spre deosebire de operatorii de servicii esenţiale, sunt liberi să ia măsuri tehnice şi organizaţionale pe care le consideră adecvate şi proporţionale pentru a gestiona riscul prezentat pentru securitatea

[22] Pentru mai multe detalii a se vedea art. 9 din Directiva NIS.

[23] Conform art. 25 alin. (3) din Legea nr. 362/2018.

sistemelor lor[24]. Art.16 alin. (1) din Directivă enumeră elementele care trebuie să fie luate în considerare de un furnizor de servicii digitale atunci când identifică şi adoptă măsuri de securitate pentru reţeaua informatică, şi anume: (a) securitatea sistemelor şi instalaţiilor, (b) gestionarea incidentelor, (c) managementul continuităţii activităţii, (d) monitorizarea, auditul şi testarea şi (e) conformitatea cu standardele internaţionale.

Adiţional cerinţelor de securitate menţionate, pentru ca furnizorii de servicii digitale să asigure un nivel ridicat de securitate a reţelei şi a sistemului său informatic, aceştia au obligaţia de a notifica orice incident cu impact substanţial asupra prestării serviciului lor[25].

Notificarea incidentelor de securitate va cuprinde, în mod obligatoriu, următoarele informaţii: a) elementele de identificare ale infrastructurii şi operatorului sau furnizorului în cauză; b) descrierea incidentului; c) perioada de desfăşurare a incidentului; d) impactul estimat al incidentului; e) măsuri preliminare adoptate; f) lista de autorităţi ale statului afectate de incident; g) întinderea geografică potenţială a incidentului; h) date despre efecte potenţial transfrontaliere ale incidentului[26].

2.3. Sancţiuni conform NIS

Conform art. 36 din Legea nr. 362/2018, la nivel naţional, controlul respectării prevederilor Directivei NIS este exercitat de Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), instituţie publică cu personalitate juridică, aflată în coordonarea Ministerului Comunicaţiilor şi Societăţii Informaţionale[27]. Începând cu data de 27 septembrie 2021, CERT-RO a fost desfiinţat, atribuţiile acestuia fiind preluate de către Directoratul Naţional de Securitate Cibernetică[28].

Legea nr. 362/2018 prezintă în cuprinsul art. 38 faptele care constituie încălcări ale cerinţelor NIS şi care, după caz, pot atrage răspunderea contravenţională sau penală. Sancţiunile prevăzute de Legea nr. 362/2018 pentru încălcarea dispoziţiilor privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice constau în aplicarea de amenzi cuprinse între 3.000 lei şi 50.000 lei, iar în cazul constatării unor încălcări repetate limita maximă a amenzii este plafonată la 100.000 lei. Întrucât valoarea pragurilor maximale ale amenzii ar putea fi considerată un risc de afaceri asumat de către marile companii, Legea nr. 362/2018 instituie pentru persoanele cu o cifră de afaceri de peste 2.000.000 lei,

[24] Conform art. 16 alin. (1) din Directiva NIS. A se vedea şi D. Markopoulou, V. Papakonstantinou, P. de Hert, *op. cit.*, p 5.

[25] A se vedea art. 16 alin. (3) și 4) din Directiva NIS.

[26] Conform art. 26, alin. (3) din Legea nr. 362/2018.

[27] Hotărârea de Guvern nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO.

[28] Ordonanța de urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, publicată în Monitorul Oficial, Partea I, nr. 918 din 24 septembrie 2021.

sancţiunea amenzii în cuantum de la 0,5% la 2% din cifra de afaceri, iar, în cazul unor încălcări repetate, amendă de până la 5% din cifra de afaceri.

3. Analiză comparativă: NIS vs. GDPR

Interacţiunea inevitabilă a prevederilor Directivei NIS cu cele ale Regulamentului GDPR este prezentată expres în cadrul capitolului 7 al Directivei.

Intrarea în vigoare a Regulamentului GDPR şi a Directivei NIS, au coincis în mare măsură, respectiv luna aprilie şi luna iulie a anului 2016. Procesele de legiferare s-au desfăşurat independent şi în paralel, neexistând o coordonare în vederea armonizării celor două reglementări. Dovadă a acestui aspect este şi art. 2 al Directivei NIS care face trimitere la Directiva 95/46/CE pentru prelucrarea datelor cu caracter personal, în loc de Regulamentul GDPR care era în vigoare la data respectivă.

În acelaşi timp, GDPR nu face nicio trimitere directă către prevederile Directivei NIS, clarificând însă, în textul considerentului nr. 49, faptul că *„prelucrarea datelor cu caracter personal în măsura strict necesară şi proporţională în scopul asigurării securităţii reţelelor şi a informaţiilor, şi anume capacitatea unei reţele sau a unui sistem de informaţii de a face faţă, la un anumit nivel de încredere, evenimentelor accidentale sau acţiunilor ilegale sau rău intenţionate care compromit disponibilitatea, autenticitatea, integritatea şi confidenţialitatea datelor cu caracter personal stocate sau transmise, precum şi securitatea serviciilor conexe oferite de aceste reţele şi sisteme, sau accesibile prin intermediul acestora, de către autorităţile publice, echipele de intervenţie în caz de urgenţă informatică, echipele de intervenţie în cazul producerii unor incidente care afectează securitatea informatică, furnizorii de reţele şi servicii de comunicaţii electronice, precum şi de către furnizorii de servicii şi tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză”.*

Cu toate acestea, lipsa recunoaşterii explicite nu înseamnă că Directiva NIS şi GDPR nu au legătură. Dimpotrivă, atâta timp cât reţelele şi sistemele informaţionale sunt utilizate pentru prelucrarea datelor cu caracter personal, ambele instrumente juridice îşi găsesc aplicare concomitent[29].

Interacţiunile între GDPR şi Directiva NIS pot apărea ori de câte ori se găsesc date cu caracter personal în sistemele furnizorilor de servicii digitale şi/sau ale operatorilor de servicii esenţiale. Un prim punct de intersecţie a celor două reglementări este reprezentat de securitatea informaţiilor, inclusiv a celor cu caracter personal. Principiul securităţii datelor cu caracter personal este unul dintre principiile de bază ale GDPR şi include principiul integrităţii şi cel al confidenţialităţii datelor, fiind menţionat în art. 5 alin. (1) lit. f) din GDPR faptul că datele trebuie *„prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate şi confidenţialitate”)”.*

[29] D. Markopoulou, V. Papakonstantinou, P. de Hert, *op. cit.*, p. 10.

În contextul expus, ne întrebăm dacă măsurile tehnice şi organizatorice pentru securitatea datelor implementate în vederea conformării la prevederile NIS sunt la nivelul „adecvat" pentru conformitatea cu prevederile GDPR şi vice-versa[30]. Considerăm că fiecare sistem informatic şi fiecare prelucrare de date trebuie analizată particular, iar în urma identificării şi evaluării riscurilor de securitate să fie implementate măsurile tehnice şi organizatorice corespunzătoare situaţiei faptice. Aşadar, nu există o garanţie asupra faptului că măsurile de securitate implementate în temeiul GDPR sunt suficiente pentru îndeplinirea obligaţiilor prevăzute de reglementările NIS şi nici vice-versa[31].

Un alt punct de interacţiune a reglementărilor NIS şi GDPR apare în situaţia unui incident de securitate care ar trebui notificat autorităţii competente din domeniul protecţiei datelor cu caracter personal, dar şi autorităţii competente din domeniul securităţii cibernetice. Având în vedere obiectul diferit al GDPR şi NIS, entităţile aflate în scenariul anterior prezentat ar trebui să notifice autorităţile competente în mod independent, respectând procedurile şi cerinţele impuse de fiecare reglementare[32].

În ceea ce priveşte termenul de notificare a incidentului de securitate, art. 33 GDPR prevede obligaţia operatorului de a notifica incidentul autorităţii de supraveghere competente fără întârzieri nejustificate şi, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta. Pe de altă parte, Directiva NIS nu prevede un termen pentru îndeplinirea obligaţiei de notificare a incidentelor, lăsând statelor membre posibilitatea de a stabili un asemenea termen. Astfel, legiuitorul român a prevăzut în cuprinsul Legii nr. 362/2018 obligaţia operatorilor de servicii esenţiale şi a furnizorilor de servicii digitale de a notifica de îndată CSIRT naţional incidentele care au un impact semnificativ asupra continuităţii serviciilor esenţiale/furnizării serviciilor digitale[33].

Asemeni prevederilor GDPR care obligă operatorii de date cu caracter personal să desemneze un Responsabil cu protecţia datelor (*Data Protection Officer* - DPO)[34], art. 10 alin. (1) lit. f) din Legea nr. 362/2018 impune operatorilor de servicii

[30] A se vedea și N. Saqib, V. Germanos, W. Zeng , L. Maglaras, *op. cit.*, pp. 17-18.

[31] Pentru similitudine a se vedea și M.D. Cole, S. Schmitz, *op. cit.*; C. Burton, *Security of personal data*, în C. Kuner, L.A. Bygrave, C. Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, p. 633.

[32] Punct de vedere susținut și de autoritatea de supraveghere a datelor cu caracter personal din Regatul Unit al Marii Britanii - Information Commissioner's Office, [Online] la https://ico.org.uk/for-organisations/the-guide-to-nis/nis-and-the-uk-gdpr/, accesat 11.11.2021. Mai mult decât atât, propunerea de Directivă NIS 2.0 prevede în art. 32 posibilitatea autorităților competente (NIS) să informeze autoritățile de supraveghere (GDPR) cu privire la încălcările obligațiilor de securitate cibernetică care implică o încălcare a securității datelor cu caracter personal. A se vedea și S. Schmitz-Berndt, S. Schiffner, *Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR*, în International Review of Law, Computers & Technology, 2021, 35:2, 101-115, DOI: https://doi.org/10.1080/13600869.2021.1885103, p. 106. C. Burton, *op. cit.*, p. 643.

[33] Conform art. 10 și art. 12 din Legea nr. 362/2018.

[34] Conform art. 37 din GDPR.

esenţiale obligaţia de a stabili mijloace permanente de contact şi de a desemna responsabilul cu securitatea reţelelor şi sistemelor informatice cu obligaţia monitorizării mijloacelor de contact.

În ceea ce priveşte regimul sancţionator, fapta prin care sunt încălcate simultan dispoziţiile GDPR şi cele NIS poate atrage amenzi administrative sau alte sancţiuni prevăzute în cele două reglementări, în mod cumulativ, acestea neexcluzându-se reciproc[35].

Este necesar a se avea în atenţie şi analizată posibilitatea unui conflict între Directiva NIS şi Regulamentul GDPR, scenariu puţin probabil, dar posibil. Doctrina de specialitate oferă în acest sens un posibil scenariu în care prevederile GDPR ar intra în conflict cu cele ale Directivei NIS[36]. Scenariul menţionat prevede situaţia în care un stat membru UE ar decide să permită operaţiuni de prelucrare a datelor cu caracter personal interzise sau strict reglementate de GDPR, ca parte a strategiei naţionale de securitate cibernetică, precum operaţiunile de profilare pe baza unor categorii speciale de date (adrese IP care provin din regiuni cu concentraţie mare de populaţii etnice sau religioase) fără asigurarea garanţiilor prevăzute de art. 22 din GDPR.

Astfel, orice suprapunere a domeniului de aplicare ar trebui rezolvată printr-o relaţie *lex specialis - lex generalis*, GDPR prevalând în cazul unui conflict cu prevederile Directivei NIS. În sprijinul acestei opinii evidenţiem faptul că atât GDPR[37] cât şi Tratatul de funcţionare a Uniunii Europene[38] includ dreptul la protecţia datelor cu caracter personal în categoria drepturilor fundamentale. Mai mult decât atât, analizând valorile sociale ocrotite de GDPR şi Directiva NIS este indubitabil faptul că protecţia datelor cu caracter personal trebuie să prevaleze securităţii cibernetice. Totodată, opinia poate fi argumentată şi prin ierarhia instrumentelor juridice potenţial conflictuale. Aşadar, Directiva NIS fiind transpusă în legislaţia naţională a fiecărui stat membru, un potenţial conflict ar

[35] Punct de vedere susținut și de autoritatea de supraveghere a datelor cu caracter personal din Regatul Unit al Marii Britanii - Information Commissioner's Office, [Online] la https://ico.org.uk/for-organisations/the-guide-to-nis/nis-and-the-uk-gdpr/, accesat 11.11.2021.

[36] D. Markopoulou, V. Papakonstantinou, P. de Hert, *op. cit*., p. 10-11.

[37] Considerentul (1) din GDPR prevede faptul că: *„Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene („carta”) și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc”.*

[38] Art. 16 TFUE prevede faptul că: *„(1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. (2) Parlamentul European și Consiliul, hotărând în conformitate cu procedura legislativă ordinară, stabilesc normele privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii, precum și de către statele membre în exercitarea activităților care fac parte din domeniul de aplicare a dreptului Uniunii, precum și normele privind libera circulație a acestor date”.*

avea loc între un Regulament UE şi o normă de drept naţională, reglementarea europeană având în mod normal prioritate.

Concluzii

Directiva NIS reprezintă un prim pas spre standardizarea nivelului minim de securitate cibernetică la nivelul operatorilor de servicii esenţiale şi a furnizorilor de servicii digitale care activează în statele membre UE. Totuşi, această etapă necesară a fost implementată cu întârziere în contextul evoluţiei tehnologiei, a răspândirii şi accesibilităţii dispozitivelor IoT şi a prelucrărilor automatizate de date.

Întrucât măsurile tehnice necesar a fi implementate de persoanele vizate de Directiva NIS pot reprezenta pentru operatorii de date cu caracter personal un model de urmat în misiunea de conformare la prevederile GDPR şi de asigurare a securităţii datelor confidenţiale, conformarea la standardele de securitate cibernetică cât mai înalte devine un deziderat pentru orice entitate care prelucrează informaţii.

Având în vedere complexitatea şi amploarea elementelor tehnice din reglementările NIS subliniem faptul că, spre deosebire de procesul de conformare la prevederile Regulamentului GDPR în care juristul avea nevoie de sprijinul unui specialist IT, implementarea standardelor de securitate impuse de Directiva NIS devine şi mai anevoioasă în lipsa unei cooperări active între echipa de specialişti IT şi jurişti.

Referinţe

Cole M.D., Schmitz S., *The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape* (December 31, 2019), în University of Luxembourg Law Working Paper No. 2019-017, http://dx.doi.org/10.2139/ssrn.3512093

Kuner C., Bygrave L.A., Docksey C., *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020

Saqib N., Germanos V., Zeng W., Maglaras L., *Mapping of the Security Requirements of GDPR and NIS*, în Preprints, iunie 2020

Schmitz-Berndt S., Schiffner S., *Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR*, în International Review of Law, Computers & Technology, 2021, 35:2, pp. 101-115, https://doi.org/10.1080/13600869.2021.1885103

Tataru Ş.R., *Internet Cookies - fişierele cu răvaş juridic*, în Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza"din Iaşi, Tomul LXVI, Supliment, Ştiinţe Juridice, 2020

Ungureanu C.T., *Contractul Cloud Computing în comerţul internaţional*, în Revista Moldovenească de Drept Internaţional şi Relaţii Internaţionale, Nr. 3 (37), 2015

Ungureanu C.T., *Drept internaţional privat european în raportul de comerţ internaţional*, Editura Hamangiu, Bucureşti, 2021

Ungureanu C.T., *Implicaţiile Internetului în viaţa juridică*, în Analele Ştiinţifice ale Universitaţii „Alexandru Ioan Cuza" Iaşi, Tomul LXIII, Ştiinţe Juridice, nr. II, 2017

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-22

Data Protection and Digital Services – European Union Perspectives

Protecţia datelor cu caracter personal şi serviciile digitale – perspective ale Uniunii Europene

Andreea Şerban[1], **Cláudio Barbosa Teixeira**[2]

Abstract: The EU is taking further steps towards the regulation of the digital space. Following on the adoption of the General Data Protection Regulation (GDPR), the European Commission now proposes two new regulation proposals aimed at regulating online markets and create a safer online environment, where the fundamental rights of users are protected: the Digital Services Act and the Digital Markets Act. However, it is still up for discussion how these proposals will articulate with GDPR provisions. In this study, we shall discuss the potential impact on data protection rules of the latest EU legislative push and how it intends to balance the new horizontal regulation for digital markets with already existing legislation, in particular on data protection.

Keywords: data protection; digital services; digital markets; online platforms; content moderation; GDPR; DSA; DMA

Rezumat: Uniunea Europeană face noi paşi pentru reglementarea spaţiului digital. În urma adoptării Regulamentului general privind protecţia datelor (GDPR), Comisia Europeană lansează două noi propuneri de regulament care vizează reglementarea mediului online, Actul legislativ privind serviciile digitale şi Actul legislativ privind pieţele digitale, cu scopul de a crea un mediu online mai sigur, în care drepturile fundamentale ale utilizatorilor să fie protejate. Cu toate acestea, există în continuare dezbateri privind modul în care prevederile acestor regulamente vor fi coroborate cu GDPR. În prezentul studiu, vom urmări potenţialul impact al noilor propuneri legislative europene asupra normelor privind protecţia datelor cu caracter personal.

Cuvinte-cheie: protecţia datelor; servicii digitale; platforme online; moderarea conţinutului; GDPR; DSA; DMA

[1] PhD candidate, Faculty of Law, “Alexandru Ioan Cuza” University of Iași, Romania, e-mail: andreeaserban20@yahoo.com.

[2] Master in European Law (LL.M.), College of Europe (Bruges, Belgium), Master of Public International Law and European Law, Universidade de Coimbra (Coimbra, Portugal), e-mail: claudio.teixeira@coleurope.eu.

1. General considerations

The General Data Protection Regulation[3] (hereinafter, the GDPR) is a landmark in the evolution of the European privacy framework[4], with a resounding global impact. The GDPR has definitely raised the bar for data protection legislations around the globe[5], effectively setting the European Union (EU) legislation and the case-law of the Court of Justice of the European Union (CJEU) as a "global gold-standard"[6] for other jurisdictions[7], with several international legislators, as well as private companies, following its lead[8].

Nonetheless, the technological and digital revolution which is currently is taking place at an ever-accelerating rate is putting into evidence that the broad scope of the GDPR is starting to grow too broad to fully cover all potential situations where personal data is processed. As Purtova[9] puts it, as the material scope of the GDPR is "bound to expand even further and, as a result, to apply to an exponentially growing range of situations", EU data protection law faces a real risk of becoming "the law of everything", which is "meant to deliver the highest legal protection under all circumstances, but in practice impossible to comply".

The GDPR guarantees the protection of personal data whenever the data is being processed, regardless of the format of the data. According to the regulation, data protection is about the rights and interests of individuals – data subjects – and

[3] 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 (General Data Protection Regulation), [Online] at https://eur-lex.europa.eu/eli/reg/2016/679/oj, accesed at 10.11.2021.

[4] M. Goddard, *The EU General Data Protection Regulation (GDPR): European regulation that has a global impact*, in International Journal of Market Research Vol. 59, Issue 6, p.703, DOI: https://doi.org/10.2501/IJMR-2017-050.

[5] G. Buttarelli, *The EU GDPR as a clarion call for a new global digital gold standard,* 2016, p. 77-78.

[6] J.P. Albrecht, *How the GDPR will change the world*, in European Data Protection Law Review. 2, 2016, p. 287; W. Veil, *The GDPR: The Emperor's New Clothes-On the Structural Shortcomings of Both the Old and the New Data Protection Law*, in Neue Zeitschrift für Verwaltungsrecht 10.2018, pp. 686-696.

[7] J. Kessler, *Data Protection in the Wake of the GDPR: California's Solution for Protecting the World's Most Valuable Resource*, in Southern California Law Review, vol. 93:99, 2019, p. 99.

[8] This "domino-effect" showcases the "Brussels Effect", how European standards become global standards not only due to mimicked legislation, but also the interest of private companies to comply with EU standards in order to access the Single Market, A. Bradford, The Brussels Effect. How the European Union rules the world. Oxford University Press, 2020.

[9] N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, in Law, Innovation and Technology, 10:1, 40-81, p. 41. DOI: https://doi.org/10.1080/17579961.2018.1452176.

not about the data relating to them[10]. Article 4 para. (1) provides us with our definition for *'personal data'*: *any information relating to an identified or identifiable natural person*, while Article 4 para. (2) defines *'processing': any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.* Therefore, any information can be considered personal data, provided that the processing of such data may refer to an identified or identifiable person. The European legislator distinguishes between personal data and non-personal data, the latter being the subject of *Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data*[11] and defined, according to its article 3, para. (1) as *"data other than personal data as defined"* in the GDPR. Although the non-personal data regulation provides obligations which are mostly directed to the Member States, these are of relevance for the private sector as well, a reminder that data should not be perceived and observed through a tunnel-vision perspective.

Overall, the purpose of the GDPR is to establish the adequate legal framework for the processing of personal data and protecting the rights of individuals, by placing a burden of responsibility and accountability on the data processors while, simultaneously, ensuring the protection of the rights of data subjects under any circumstance, including potential situations which are not yet provided for by the GDPR, a future-proofing element given the continuous technological advancements and the absence of immediate legislative responses.

Just how sufficient is the GDPR and how successful has it been so far? In the GDPR third anniversary communication, the European Data Protection Supervisor (hereinafter, the EDPS) acknowledged that "the GDPR has been a sensational achievement for Europe and its citizens, acting as a lighthouse for the entire global policy-making scene and illuminating long-held privacy and data protection values enshrined across the horizon of the European legislative landscape. It has acted as a catalyst for many jurisdictions around the world to draft and implement their own privacy and data protection legislation"[12].

The GDPR granted data protection authorities with extended competences to curb the unlawful data power and enforce privacy rules and the rule of law.

[10] P. Hustinx, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, p. 1, [Online] at https://edps.europa.eu/sites/default/files/publication/14-09-15_article_eui_en.pdf, accessed at 10.11.2021.

[11] 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, [Online] at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807, accessed at 10.11.2021.

[12] W. Wiewiorowski, *GDPR: a three-year old who must still learn to walk before it runs*, [Online] GDPR: a three-year-old who must still learn to walk before it runs | European Data Protection Supervisor (europa.eu), accessed at 10.11.2021.

Though, it is rather questionable just how far do the extended powers of national authorities go in enforcing GDPR. Such fears can be illustrated by the latest track record of Ireland, the Member State that hosts some of the biggest actors that process personal data in the EU[13]. The Irish Data Protection Commission (hereinafter, DPC) catches the attention of other GDPR enforcers, as the decisions by the DPC have the potential to set relevant precedents of practice and legal interpretation in this still-young field of practice. However, the most recent (leaked) draft decision on Facebook[14], the DPC has set a questionable precedent, for several reasons: on the one side, at first sight, this decision that was shared with other EU data protection authorities potentially provides cover for a Facebook legal trick aimed at, essentially, *bypassing the GDPR*[15]. In the view of the DPC in its draft decision, "there is no obligation on Facebook to seek to rely solely on consent for the purposes of legitimizing personal data processing where it is offering a contract to a user which some users might assess as one that primarily concerns the processing of personal data". Facebook can therefore simply choose to include the agreement on data processing in a contract which would make the GDPR requirements for consent not apply anymore. Yet, the authority suggests (only) a penalty of 28 to 36 million EUR as "Facebook ought to have been more transparent on this bypass"[16].

Has the GDPR achieved its purpose? Should we consider the protection of the rights of the data subject in relation to the processing of their personal data, then indeed it has. The above-mentioned general framework ensures said protection in any potential situation of data processing. Given the direct effect of a EU regulation, directly and immediately enforceable in Member States, GDPR has achieved the quite visible purpose of setting standardized data protection rules across the EU and even realizing a secondary purpose of triggering an awareness movement that made inroads in educating the general population on their privacy and data rights. Indeed, when it comes to its impact on the private sector, the GDPR provided for considerable changes to the privacy protection by fostering compliance by private companies, from the necessity to review their strategy to reassessing their information systems and documentation in order to ensure compliance with the new provisions in order to freely trade with and within the Single Market[17].

[13] For example, Twitter International Company, Facebook, Google and so on.

[14] See the draft decision published [Online] at www.noyb.eu: https://noyb.eu/sites/default/files/2021-10/IN%2018-5-5%20Draft%20Decision%20of%20the%20IE%20SA.pdf, accessed at 14.10.2021.

[15] Irish DPC greenlights Facebook's "GDPR bypass". *Irish DPC greenlights Facebook's "GDPR bypass". Schrems: "Decision undermines key element o GDPR"*, [Online] at https://noyb.eu/en/irish-dpc-greenlights-facebooks-gdpr-bypass, accessed at 14.10.2021.

[16] *Ibidem.*

[17] C. Tikkinen-Piri, A. Rohunen, J. Markkula, *EU General Data Protection Regulation: Changes and implications for personal data collecting companies*, in Computer Law & Security Review, Vol. 34, Issue, 1, February 2018, p. 134-153.

Yet is the GDPR the only go-to piece of legislation when it comes to the continuously improving technologies and their impact on the processes related to personal data? Definitely not. Just as the Directive 95/46[18], the precursor of the GDPR, eventually ceased to adequately respond to the regulatory needs of a rapidly changing and evolving technological reality of constant technological developments, it is curious to observe that, almost two decades later, the GDPR starts to find itself in a similar situation. While the first act is a Directive, therefore leaving room for implementation by Member States, in its turn the GDPR is calling for additional legislative acts which will complement and provide a more in-depth framework, depending on the legislative needs correlated to the emerging technologies. For example, its broadened material scope and generalized – or rather stand-alone – provisions have raised more questions than provided answers; questions which have eventually been brought before the CJEU for further clarifications – one of the latest examples in this regard, the Schrems II decision[19], indeed invalided the European Commission's Privacy Shield Decision[20], determining a period of legislative gap in terms of transfers of personal data between the EU and the United States of America, and, later, the adoption of new sets of standard contractual clauses[21].

We can therefore conclude thus far that the GDPR stands as a comprehensive legal framework, which covers multiple situations where personal data is processed. Nonetheless, it is not a catch-all legislation, with several shortcomings having been identified over its tenure in force. However, one of the most pressing concerns has become the challenge of online platform economy and processing and monetisation of data.

[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [Online] at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046, accessed at 14.10.2021.

[19] Judgement of the Court of 16 July 2020, in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems.*

[20] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, [Online] at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG, accessed at 14.10.2021.

[21] Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, [Online] at https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj, accessed at 14.10.2021. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, [Online] at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, accessed at 14.10.2021.

2. The challenge of online platform economy: data collection and monetization

The GDPR was adopted at a time when it became more and more clear that personal data has become over the past decades "a critical source of innovation and value", and the business boundaries[22] keep being redrawn. Personal data has become an extremely valuable commodity, as the online platform economy took off based on an advertised-based business model. Data provides relevant information to companies about people's interests and activities, and thus offering a relevant basis for personalized advertising, but not only. The companies that provide services on the Internet are built on the economics of personal data[23].

Personal data is now an economic asset – the identities and online behaviours of data subjects is traded in exchange for services and products of higher quality[24]. The monetization of personal data is a reality, and it has been identified as a relevant aspect of the new market for consumer's data, given the fact that individuals have a broad access to digital services[25]. It provides an "advantage" to the consumers of the digital services, usually found in at least three forms: (1) "free" or discounted provision of online services – such as wifi access in public spaces by accepting the cookies and trackers and providing an email address in exchange of free Internet navigation; (2) "free" or discounted provision of (valuable) online content – such as access to music platforms that provide all kind of songs and music content, even if protected by copyright, for free, in exchange of the creation of a profile which contains personal data such as email address and, in certain cases, the profile used on other social media platforms; (3) "free" or discounted provision of an "offline" service – such as insurance[26].

[22] World Economic Forum, *Personal Data: the emergence of a new asset class*, January 2011, [Online] at https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf, accessed at 20.11.2021.

[23] A. Esteve, *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, in International Data Privacy Law, 2017, Vol. 7, no. 1, p. 36.

[24] C. Liem, G. Petropoulos, *The economic value of personal data for online platforms, firms and consumers,* blog post, January 2016, [Online] The economic value of personal data for online platforms, firms and consumers | Bruegel, accessed at 20.11.2021.

[25] "Different platforms collect and monetize data in various ways: either through a direct subscription model (e.g. Spotify)—by using collected data to tailor products directly to users (e.g. Amazon)—or by selling targeted ads (e.g. Facebook and Google Search). Most zero-price ad-based platforms use the latter business model, enabling them to establish market power in the complementary positive-price digital advertising market." B. Kira, V. Sinha, S. Srinivasan, *Regulating digital ecosystems: bridging the gap between competition policy and data protection, Industrial and Corporate Change*, in Industrial and Corporate Changes, 2021, 00, 1-24, DOI: https://doi.org/10.1093/icc/dtab053.

[26] G. Malgieri, B. Custers, *Pricing privacy: the right to know the value of your personal data*, in Computer Law & Security Review, 2017, p. 5-6.

Directive (EU) 2019/770 on contracts for the supply of digital content and digital services[27] acknowledged that, in the modern digital economy, personal data can be used as payment for digital content, instead of money. Its recital 24 states that "digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market". It further stipulates that "while fully recognizing that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies". In its article 3 para. (1), the Directive states that it applies "to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price", including when "the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader", with the exception where "the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose". Although the price, for the purposes of this Directive, is defined in art. 1 (7) as "money or a digital representation of value that is due in exchange for the supply of digital content or a digital service" and personal data is understood as it is defined by the GDPR, the conclusion is that the equation of personal data in exchange for "free" digital content has the same result as the one regarding money in exchange for paid digital content, which is the provision of digital services to consumer, such as provision of access to the consumer of digital content.

The discussion on privacy and data protection has opened a veritable *Pandora's Box*. The GDPR is a legislative instrument that protects personal data, although it remains insufficient to cover all aspects of the processing of data, given this being an on-going learning process, constantly adapting to the development of technologies and digital realities. Any type of data, either personal or non-personal, is tradable[28] and the data market is ever growing. The digital space provides the environment for experimenting with situations and outcomes of data processing which must be addressed by the legislator to provide a legal basis to the upcoming realities.

From the identified GDPR shortcomings, given the rapidly evolving technological landscape, the most pressing for EU legislators at this moment seems to be the need to provide adequate protection of the data subject in relation to their

[27] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, [Online] at https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX: 32019 L0770/, accessed at 20.11.2021.

[28] For further detailing of the trade with data, see C.T Ungureanu, *Drept international privat european in raporturi de comert international*, Hamangiu, 2021, pp. 117-125.

personal data on the Internet, where any information relates to a person in the sense of EU data protection law. At a time when the online platform economy processes and monetises data in exchange of providing digital services, which are highly optimised to benefit advertising-driven business models relying, in turn, on advanced data analytics and data-driven decision-making systems, the challenge of the increase of targeted profiling and automated decision-making techniques which depend on the processing of personal data, mostly obtained via applications of extremely intrusive nature[29], requires an adequate and complementary response from the European legislator. The response of the current European legislative agenda so far? The Digital Services Act package.

3. The Digital Services Act package

In December 2020, as a part of the Digital Services legislative package, the European Commission presented two new legislative proposals[30], the Digital Services Act (DSA) and the Digital Markets Act (DMA), new *ex ante* horizontal legislation to govern digital services "applicable across the whole EU to create a safer and more open digital space". The legislative procedure on these proposals is still ongoing therefore our analysis will naturally focus on the original proposal[31].

In general terms, the proposals bear a strong influence from the GDPR and share elements in common[32]. While the GDPR has laid down the main principles of transparency, fairness and lawfulness, which apply to all kinds of personal data processing activities - including online platforms – the DSA and DMA proposals bring their added value to the table by elaborating on these principles while introducing a specific regulatory framework for digital platforms. Therefore, the interplay between GDPR, on the one hand, and the DSA and DMA proposals, on the other hand, is of extreme importance to ensure effective complementarity of the data protection rules.

[29] S. Hänold, *Profiling and Automated Decision-Making: Legal Implications and Shortcomings,* in M. Corrales, M. Fenwick, N. Forgó, (eds) Robotics, AI and the Future of Law in Perspectives in Law, Business and Innovation, Springer, Singapore, https://doi.org/10.1007/978-981-13-2874-9_6.

[30] The DSA and DMA are still draft proposals by the European Commission which, at the time of this article, are still under discussion by the EU co-legislators, the European Parliament and the Council of the EU, whose position is awaited until the end of year of 2021, with interinstitutional negotiations aimed at achieving a final agreement expected to take place in early 2022.

[31] See European Commission, *The Digital Services Act package*, [Online] at https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package, accessed at 15.11.2021.

[32] A. Gascón Macén, *El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea*, Cuadernos de Derecho Transnacional, 13(2), 209-232, https://doi.org/10.20318/cdt.2021.6256.

The Commission clarified on both proposals that the future regulations will complement of data protection rules "without prejudice of their application"[33], namely GDPR and the E-Privacy Directive (Directive 2002/58/EC)[34]. The fact that the proposal seeks to complement, rather than to replace the GDPR, was welcomed by the European Data Protection Supervisor (EDPS), having considered that, in the context of the online platform economy, "competition, consumer protection and data protection law are three inextricably linked policy areas"[35], that should have a relationship of complementarity and not of overlapping, "where one area replaces or enters into friction with another"[36].

4. Brief considerations on the Digital Services Act proposal

4.1. Context

The DSA proposal lays down rules and obligations for intermediary service providers, including platforms and hosting services[37] (i.e., online marketplaces, social networks, app stores, content-sharing, travel, and accommodation platforms), having a special focus on protecting users from illegal activities online and increase transparency for online platforms. More importantly, "very large online platforms" (VLOPs)[38], will have additional obligations: thresholds for designation as a VLOP and falling under such additional obligations is currently estimated as serving more than 45 million service recipients within the EU. This threshold should be adjusted by the Commission so that it consistently corresponds to 10% of the EU population[39].

[33] Article 1 (5), recitals 9 to 11, of the DSA proposal; recital 11 of the DMA proposal.

[34] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [Online] at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri= CELEX%3A32002L0058, accessed at 15.11.2021.

[35] *Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, March 2014, [Online] at https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf, accessed at 15.11.2021.

[36] European Data Protection Supervisor, Opinion 1/2021, on the Proposal for a Digital Services Act, p. 3, [Online] at https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf, accessed at 15.11.2021.

[37] Proposal of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, [Online] at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en, accessed at 15.11.2021.

[38] Such as the commonly known "Big Four" or GAFA: Google, Apple, Facebook, Amazon.

[39] Proposal of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, [Online] at https://eur-

In its Opinion 1/2021, the EDPS confirmed that the DSA proposal "will clearly have an impact on processing of personal data", considering it "necessary to ensure complementarity in the supervision and oversight" of platforms and other providers. Moreover, given the "already endemic monitoring of individuals' behavior, in particular on online platforms"[40], the supervisor recognised that "certain activities in the context of online platforms present increasing risks not only for the rights of individuals, but for society as a whole"[41].

4.2. Online advertising, recommender systems

And what are said risks? In the context of "surveillance capitalism"[42], the advertising industry provides the major incentive towards the collection and selling of personal data. The increase of profiling and automated decision-making techniques which depend on the processing of personal data can lead to the uncontrolled spread of illegal content, harmful content (such as disinformation), discrimination and privacy violations[43]. Regulators are starting to catch-up to the need to address the issue: recently, the United Kingdom's Competition and Markets Authority (CMA) has called for a "right not to be profiled", or the "choice requirement"[44].

The EDPS has equally revealed its concern on its Opinion on the DSA proposal, where it concluded that, in order to ensure complementarity with the GDPR, the proposal requires additional safeguards, making specific recommendations against profiling and tracking on content moderation, online targeted advertising (articles 24 and 30) and recommender systems (article 29)[45].

Regarding online advertising, the supervisor comes out in support a future ban on targeted tracking-based advertising, asking for a "phase-out leading to a prohibition of targeted advertising on the basis of pervasive tracking" and for stricter regulation "in favour of less intrusive forms of advertising that do not

lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en, accessed at 15.11.2021.

[40] European Data Protection Supervisor, Opinion 1/2021, on the Proposal for a Digital Services Act, p. 13

[41] *Idem*, p. 3.

[42] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2019.

[43] S. Hänold, *Profiling and Automated Decision-Making: Legal Implications and Shortcomings,* in M. Corrales, M. Fenwick, N. Forgó, (eds) Robotics, AI and the Future of Law in Perspectives in Law, Business and Innovation. Springer, Singapore, https://doi.org/10.1007/978-981-13-2874-9_6.

[44] Competition and Markets Authority (CMA), United Kingdom, Online platforms and digital advertising, July 2020, 8.90, p. 379, [Online] at https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf, accessed at 15.11.2021.

[45] European Data Protection Supervisor, Opinion 1/2021, on the Proposal for a Digital Services Act, p. 3.

require any tracking of user interaction with content"[46]. In addition, it recalled the risks of profiling and micro-targeting in the context of recommender systems[47], noting that article 29 para. (1) of the DSA proposal should comply with the requirements of data protection by design and by default set out in Article 25, GDPR: recommender systems should by default not be based on "profiling", as defined in Article 4 para. (4) GDPR. Article 29 para. (1) of the DSA proposal should therefore provide for an opt-in, instead of an opt-out on profiling.

In summary, the EDPS has stated that transparency measures alone will not sufficiently address the risks posed by targeted tracking-based advertising; non-profiling by default should therefore be the default option for legislators, by prohibiting surveillance advertising and profiling-based recommender systems.

4.3. Supervision and enforcement

One of the main identified shortcomings of the application of EU data protection rules is their enforcement. The experience of GDPR enforcement has put into questioning the efficiency of the one-stop-shop approach and the "country-of-origin principle", where supervision and enforcement powers first rely with national regulatory authorities of Member States where the companies are established. Given that most of the major technological companies covered by the scope of this legislation finds its headquarters in only a limited number of Member States, such as Ireland or Luxembourg, cross-border enforcement bottlenecks remain a significant challenge: in Ireland, the Irish Civil Liberties Council (ICCL) has revealed that about 98% of major GDPR cases referred to the Irish Data Protection Commission (DPC) remain unresolved[48].

Justice delayed is justice denied[49]. Should the new legislation aim to adequately complement GDPR, it would go a long way in addressing enforcement bottlenecks. However, the DSA proposal maintains the preference for the "country-

[46] European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market, P9_TA(2020)0272, [Online] at https://www.europarl.europa.eu/doceo/document/ TA-9-2020-0272_EN.pdf, accessed at 15.11.2021.

[47] See European Data Protection Supervisor, "Opinion 3/2018 EDPS Opinion on online manipulation and personal data", 19 March 2018, p. 9, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf ("Manipulation also takes the form of microtargeted, managed content display which is presented as being most 'relevant' for the individual but which is determined in order to maximize revenue for the platform. This is akin to the 'secret menus' used to steer users of ecommerce sites and the 'dark patterns' used to dissuade decisions less desirable from the platform's perspective (such as declining to add additional items, like insurance, to a shopping cart").

[48] Irish Civil Liberties Council, 2021 report on the enforcement capacity of data protection authorities, [Online] at https://www.iccl.ie/news/2021-gdpr-report/, accessed at 15.11.2021..

[49] N. Burstyner, T. Sourdin, *Justice Delayed is Justice Denied*, in Victoria University Law and Justice Journal, 4(1), October 2014, DOI: https://doi.org/10.15209/vulj.v4i1.61.

of-origin principle"[50], thus sharing a similar enforcement model with GDPR and raising pertinent questions whether enforcement issues will remain.

5. Brief considerations on the Digital Markets Act proposal

Personal data is a source of market power: this data-driven advantage of large platforms derives from their access, collection and monetisation of users' personal data on an industrial scale, from all kinds of sources and backgrounds[51]. Moreover, this advantage amounts to market entry barriers for entry-level competitors, as large online platforms that play a systemic role in the market become entrenched.

To ensure digital markets are fairer and more contestable, the DMA proposal sets out *ex ante* horizontal rules, creating obligations for the designated "gatekeepers"[52]: a new definition which applies to large online platforms, with a strong economic position with significant market impact, a strong intermediation position or an entrenched and durable position in the market[53]. The DMA in the proposed form sets out provisions concerning the designation of gatekeepers of the service provider while providing the core platform services as well as other digital services.

In its current form, the DMA may affect the following eight categories of core platform service: (1) social media networks, (2) search engines, (3) video platforms, (4) communication services, (5) intermediation services, (6) cloud computing services, (7) operating systems, and (8) advertising networks that operate alongside any of the above. To qualify as gatekeeper, the following criteria is considered: (1) 45 million monthly users (around 10% of the EU population), (2) global turnover of or exceeding 6,5 billion EUR, and (3) operations in at least 3 of the 27 EU Member States, according to Article 3 of the DMA proposal. The criteria for designation of these "gatekeepers" has been called out[54] for their legal certainty and accountability, as well as proportionality issues that are raising in their current form.

While the GDPR has met shortcomings when addressing the importance of data for competition, the proposal on DMA attempts to respond to this issue: gatekeepers may not combine personal data from different sources, and the DMA

[50] Article 40, Proposal on Digital Services Act (DSA)

[51] B. Kira, V. Sinha, S. Srinivasan, *Regulating digital ecosystems: bridging the gap between competition policy and data protection, Industrial and Corporate Change*, in Industrial and Corporate Changes, 2021, 00, 1-24, https://doi.org/10.1093/icc/dtab053.

[52] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (DMA), Article 5, [Online] at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC 0842&from= en, accessed at 15.11.2021.

[53] DMA proposal, Explanatory Memorandum, p. 1, [Online] at https://eur-lex. europa. eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en, accessed at 15.11.2021.

[54] Digital Europe, *Digital Markets Act position paper*, [Online] at https:// www. digitaleurope.org/resources/digital-markets-act-position-paper/, accessed at 29.11.2021.

may offer real-time data portability to both business and individuals-users of the platforms, real-time data access to business users, and personalized search engine data[55]. The DMA thus reinforces the GDPR and complements it at competition level.

In its Opinion 2/2021[56], the EDPS also provided specific recommendations for the DMA proposal to effectively complements the GDPR. For example, it recommended specifying in Article 5(a) of the DMA proposal that the "gatekeeper shall provide end-users with a solution of easy and prompt accessibility for consent management"; clarifying the scope of the data portability envisaged in the DMA proposal.

Final considerations

The DMA and DSA have met a generally welcoming view from the EU Member States so far, as well as, for example, the European Data Protection Supervisor as mentioned above, though, being still in the draft from, it raises some questionable provisions that could be considered either too vague or in need of rewriting and amending.

Given the fact that they are still subject to discussions at the EU institutions level and the civil society organizations are advocating for clearer provisions, it is to be expected that the final form of the two proposals, if adopted, to be modified at least partially. Nonetheless, the discussion provided by the DMA and DSA proposals is welcome as it complements the privacy and data protection activity undertaken at the European level and beyond.

The GDPR alone, as shown, has blind spots that only specifically tailored legislation could clarify the situations raised in practice. The final agreed versions of the above-discussed legislative proposals should either provide these answers or raise even more questions.

Reference list

Albrecht J. P., *How the GDPR will change the world*, in European Data Protection Law Review. 2, 2016, DOI: https://doi.org/10.21552/EDPL%2F2016%2F3%2F4

Blankerts A., Jaursch J., *What the European DSA and DMA proposals mean for online platforms*, January 2021

Bradford A., *The Brussels Effect. How the European Union rules the world*, Oxford University Press, 2020

Burstyner N., Sourdin T., *Justice Delayed is Justice Denied*, in Victoria University Law and Justice Journal, 4(1), October 2014, DOI: https://doi.org/10.15209/vulj.v4i1.61

Buttarelli G., *The EU GDPR as a clarion call for a new global digital gold standard,* 2016

[55] A. Blankerts, J. Jaursch, *What the European DSA and DMA proposals mean for online platforms*, January 2021, [Online] at https://www.brookings.edu/techstream/what-the-european-dsa-and-dma-proposals-mean-for-online-platforms/, accessed at 29.11.2021.

[56] European Data Protection Supervisor, Opinion 2/2021 on the Proposal for a Digital Markets Act, [Online] at https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_ markets_act_en.pdf, accessed at 29.11.2021.

Esteve A., *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, in International Data Privacy Law, 2017, Vol. 7, no. 1, DOI: https://doi.org/10.1093/IDPL%2FIPW026

Gascón Macén A., *El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea*, Cuadernos de Derecho Transnacional, 13(2), DOI: https://doi.org/10.20318/cdt.2021.6256

Goddard M., *The EU General Data Protection Regulation (GDPR): European regulation that has a global impact*, in International Journal of Market Research Vol. 59, Issue 6, DOI: https://doi.org/10.2501%2FIJMR-2017-050

Hänold S., *Profiling and Automated Decision-Making: Legal Implications and Shortcomings*, in M. Corrales, M. Fenwick, N. Forgó, (eds) Robotics, AI and the Future of Law in Perspectives in Law, Business and Innovation, Springer, Singapore

Hustinx P., *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*

Kessler J., *Data Protection in the Wake of the GDPR: California's Solution for Protecting the World's Most Valuable Resource*, in Southern California Law Review, vol. 93:99, 2019

Kira B., Sinha V., Srinivasan S., *Regulating digital ecosystems: bridging the gap between competition policy and data protection, Industrial and Corporate Change*, in Industrial and Corporate Changes, 2021, 00, 1-24

Liem C., Petropoulos G., *The economic value of personal data for online platforms, firms and consumers*, blog post, January 2016

Malgieri G., Custers B., *Pricing privacy: the right to know the value of your personal data*, in Computer Law & Security Review, 2017

Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, in Law, Innovation and Technology, 10:1, 40-81, DOI: https://doi.org/10.1080/17579961.2018.1452176

Tikkinen-Piri C., Rohunen A., Markkula J., *EU General Data Protection Regulation: Changes and implications for personal data collecting companies*, in Computer Law & Security Review, Vol. 34, Issue, 1, February 2018, DOI: https://doi.org/10.1016/J.CLSR.2017.05.015

Ungureanu C.T., *Drept international privat european in raporturi de comert international*, Hamangiu, 2021

Veil W., *The GDPR: The Emperor's New Clothes-On the Structural Shortcomings of Both the Old and the New Data Protection Law*, in Neue Zeitschrift für Verwaltungsrecht 10.2018

Wiewiorowski W., *GDPR: a three-year old who must still learn to walk before it runs*

Zuboff S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2019

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-23

Dreptul Algoritmic

Algorithmic Law

Silvia Uscov[1]

Rezumat: Dreptul este un set de reguli de convieţuire socială, aşa încât este firesc să ne putem întrebarea dacă normele juridice pot fi „traduse” într-un limbaj de programare care să ofere soluţia algoritmică la o problemă juridică. „Dacă” răspunsul este pozitiv, „atunci” care sunt limitele acestei noi posibilităţi, evaluând potenţialele riscuri pe care le implică o astfel de operaţiune. Dreptul Algoritmic este o noţiune-umbrelă care defineşte ansamblul normativ creat de un sistem algoritmic, cu intervenţie umană minimă, pe baza datelor din viaţa reală.

Cuvinte-cheie: drept algoritmic; normativ algoritmic; inteligenţă artificială; imperativul cuantic; proces democratic

Abstract: The law is a set of rules of social coexistence, so it is natural to ask ourselves whether legal rules can be “translated” into a programming language that provides the algorithmic solution to a legal problem. “If” the answer is positive, “then” what are the limits of this new possibility, assessing the potential risks involved in such operation. Algorithmic law is an umbrella notion that defines the normative set created by an algorithmic system, with minimal human intervention, based on real life data. Algorithmic law is an umbrella notion that defines the normative set created by an algorithmic system, with minimal human intervention, based on real life data.

Keywords: algorithmic law; algorithmic normative; artificial intelligence; quantum imperative; democratic process

1. Noţiuni de bază în domeniul inteligenţei artificiale

Clifford A. Pickover[2] ilustrează istoria preocupărilor umane ce stau la baza dezvoltării în prezent a inteligenţei artificiale, plecând de la inventarea jocului „X şi 0” *(Tic-Tac-Toe)* în anul 1.300 î.Hr. şi trecând prin mitologia greacă unde avem o reprezentare a unui automaton, Talos, dar şi prin concepţia lui Aristotel în Politica, „căci dacă oricare dintre unelte, fie la poruncă, fie din presimţire, şi-ar îndeplini lucrul său, precum se spune despre statuile lui Dedal – şi despre trepiedurile lui Hefaistos, despre care poetul zice că «pătrundeau automate în ceata zeilor», dacă

[1] Avocat, Baroul Bucureşti, e-mail: silvia.uscov@uscov.eu.

[2] C.A. Pickover, *Artificial Intelligence – An Illustrated History, From Medieval Robots to Neural Networks*, Editura Sterling Publishing Co., Inc, New York, 2019.

suveicile ar ţese singure şi plectrul ar cânta singur, patronilor nu le-ar mai trebui lucrători şi nici stăpânilor, sclavi"[3,4].

Jeff Krimmel spunea că, în condiţiile în care inteligenţa artificială se defineşte ca orice tehnologie care ajută omul să ducă la îndeplinire o sarcină cognitivă, preluându-i în parte sau în tot această sarcină, atunci totul a început cu calendarul, care ne ajută să nu mai apelăm la memorie pentru calcularea zilelor, săptămânilor, anilor, şi cu abacul, care ne ajută la efectuarea unor calcule complexe[5].

Probabil că această definiţie este cea mai cuprinzătoare, deoarece arată dorinţa omenirii de a-şi augmenta capacitatea de procesare a informaţiilor, dar, prin raportare la stadiul actual de dezvoltare al tehnologiei informaţiei, care permite ca procesarea unei cantităţi uriaşe de date să fie realizată în mod automat, omului nerevenindu-i decât misiunea de a prelua rezultatul pentru a-l integra în alte procese cognitive, e nevoie de o desprindere a definiţiei de trecut şi de introducerea ei doar în sfera computerizării pentru a avea o reprezentare mai apropiată de realitate a perspectivelor viitorului.

Conform art. 3 pct. 1 din Propunerea pentru un Regulament al Parlamentului European şi al Consiliului de stabilire a unor norme armonizate privind inteligenţa artificială (Legea privind Inteligenţa Artificială) şi de modificare a anumitor acte legislative ale Uniunii (Propunerea de Regulament AI), sistemul de inteligenţă artificială este definit ca *un software care este dezvoltat prin una sau mai multe dintre tehnicile şi abordările enumerate în anexa I şi care, pentru un anumit set de obiective definite de om, poate genera rezultate precum conţinuturi, previziuni, recomandări sau decizii care influenţează mediile cu care interacţionează*[6].

Abordările menţionate în Anexa 1 se referă la Machine Learning (învăţare automată) – supervizat sau nesupervizat – şi Deep Learning (sau alte metode de învăţare aprofundată), dar şi la abordări statistice, estimări *bayeziene*, metode de căutare şi de optimizare, abordări bazate pe logică şi cunoaştere, inclusiv reprezentarea cunoştinţelor, programare inductivă (logică), baze de cunoştinţe,

[3] Aristotel, *Politica*, redactor N. Năstase, ediţie actualizează a lucrării *Politica* apărută la Editura Cultura Naţională în anul 1924, traducere de El. Bezdechi, Editura Biblioteca Centrală Universitara „Lucian Blaga", p. 8, [Online] la https://www.scribd.com/doc/25315388/Aristotel-Politica, accesat 22.11.2021.

[4] A se vedea şi M. Devecka, *Did the Greeks Believe in their Robots?*, The Cambridge Classical Journal, Volumul 59, Editura Cambridge University Press, Decembrie 2013, pp. 52 – 69, [Online] la https://www.cambridge.org/core/journals/cambridge-classical-journal/article/did-the-greeks-believe-in-their-robots/5DBC2382196660C31F8269227B05D883, accesat 22.11.2021.

[5] J. Krimmel, *Artificial Intelligence Started with the Calendar and Abacus*, 2017, [Online] la https://web.archive.org/web/20171122023732/http://www.stemtobusiness.com/artificial-intelligence-started-with-the-calendar-and-abacus, accesat 22.11.2021.

[6] Propunerea pentru un Regulament al Parlamentului European şi al Consiliului de stabilire a unor norme armonizate privind inteligenţa artificială (Legea privind Inteligenţa Artificială) şi de modificare a anumitor acte legislative ale Uniunii, COM/2021/206 final, Bruxelles, 21.04.2021, [Online] la https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206, accesat 24.11.2021.

motoare inductive şi deductive, sisteme de raţionament (simbolic) şi de expertiză *(reasoning and expert systems).*

Aceste tehnici permit unui sistem AI să înveţe cum să atingă anumite scopuri stabilite de operator *(coder)*, în cadrul cărora se cunoaşte că problemele cu care se va confrunta sistemul pentru atingerea acestor scopuri nu pot fi precis definite, presupunând analize interconectate ale căror metode nu pot descrise prin reguli de raţionament simbolic şi fiind este necesar să i se acorde sistemului o libertate mai mare de mişcare sau, am putea spune, de „gândire".

„Inteligenţa artificială (AI) se referă la sistemele concepute de oameni care, în urma stabilirii unui scop complex, acţionează în lumea fizică sau digitală prin perceperea mediului lor, interpretarea datelor structurate sau nestructurate colectate, formarea raţionamentului pe baza cunoştinţelor derivate din aceste date şi fundamentarea deciziilor celor mai adecvate privind măsurile de întreprins (conform parametrilor predefiniţi) pentru atingerea scopului dat. Sistemele AI pot fi, de asemenea, proiectate pentru a învăţa să-şi adapteze comportamentul, analizând modul în care mediul este afectat de acţiunile lor anterioare.

Ca disciplină ştiinţifică, AI include mai multe abordări şi tehnici, cum ar fi Machine Learning (din care *Deep Learning* şi *Reinforcement Learning* – învăţare consolidată – sunt exemple specifice), raţionamentul automat (care include planificarea, programarea, reprezentarea şi raţionalizarea cunoştinţelor, căutarea şi optimizarea) şi robotică (care include controlul, percepţia, senzorii şi actuatorii, precum şi integrarea tuturor celorlalte tehnici în sistemele cyber-fizice)"[7].

Pentru a se înţelege relaţia de la întreg la parte între sistemele descrise mai sus, apelăm la următoarea reprezentare grafică:

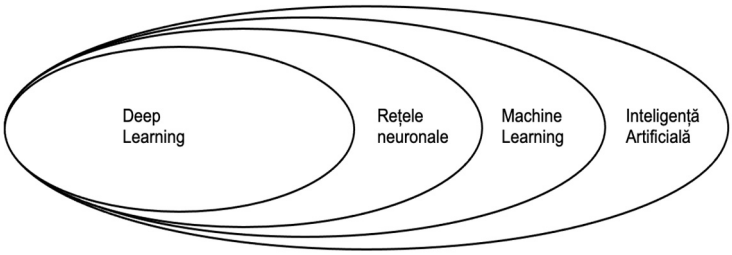

Fig. 1. Matryoshka – De la inteligenţă artificială la deep learning[8]

Acestea nu ar putea fi posibile în lipsa Big Data, care, în concepţia profesorului Ana Nordberg, „nu sunt doar seturi de date statice, printre altele, se

[7] Comisia Europeană, Directoratul General pentru Comunicare, High-Level Expert Group on Artificial Intelligence, *A definition of AI: Main capabilities and scientific disciplines*, Comisia Europeană, B-1049 Bruxelles, 18.12.2018, [Online] la https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf, accesat 25.11.2021.

[8] A se vedea [Online] https://apmonitor.com/do/index.php/Main/DeepLearning, accesat 25.11.2021

caracterizează prin faptul că sunt date eterogene în timp real, aflate în actualizare constantă şi, de asemenea, capabile să genereze în mod continuu date noi. (...) Noţiunea de Big Data este de obicei asociată şi caracterizată prin prezenţa celor «4V» – volum, viteză, varietate şi veridicitate. Volumul, se referă la un volum exploziv de date produse din diferite surse: internetul lucrurilor (n.a. IoT), reţelele sociale, aplicaţiile, senzori, reţele interne (de ex. sisteme de facturare, urmărire a mărfurilor în tranzit şi a livrărilor clienţilor); depozite de informaţii (de exemplu, baze de date, biblioteci, depozite ştiinţifice şi bio-bănci); informaţia din sectorul public etc. Viteza se referă la natura dinamică a datelor mari. Informaţiile sunt procesate în timp real şi accesate în timp ce noi date sunt produse în mod constant. Varietate, se referă la faptul că datele mari sunt date din mai multe surse, în diverse tipuri şi formate (de exemplu, imagini, texte, audio, video, comunicare nonverbală, cum ar fi *emoji*, *meme*, *hashtag*-uri, etichete, aprecieri, glisări, localizare geografică, timp, etc). Veridicitatea, corespunde nevoii ca informaţia (informaţie semantică) să fie corectă (cel puţin în lumina stadiului tehnicii). Nu toate Big Data vor cuprinde acest ultim element. Veridicitatea este un aspect căruia informaticienii îi acordă o atenţie considerabilă, în special în aplicaţiile de luare a deciziilor asistate sau automatizate (de exemplu, în sectorul judiciar sau al sănătăţii), dar şi în industria de automatizare şi auto (de exemplu, robotică şi vehicule fără şofer). Afirmarea veridicităţii datelor sursă şi de instruire necesită un control strict asupra originii acestora şi exclude multe surse de date. Nu numai că este dificil să se afirme veridicitatea datelor sursă, dar veridicitatea joacă un rol în extragerea datelor (n.a. *data mining*), şi în deducţiile (n.a. *inference*) pe baza datelor în *machine learning*. Acest tip de produs de date poate fi extrem de util în materializarea unei varietăţi de procese de luare a deciziilor, dar veridicitatea sa este extrem de dificil sau durează mult pentru a fi confirmată manual de către om. (...) Pe scurt, Big Data corespunde agregării marilor seturi de date, prelucrate prin mijloace computerizate”[9].

Prin urmare, aşa cum putem observa, problema în ceea ce priveşte Big Data nu este legată de volum, viteză sau varietate datelor, ci de calitatea acestor date, respectiv cât de corecte (veridice) sunt ele, lucru important nu numai în prima etapă, de extragere şi introducere în sistem a acestor date, ci şi de instruire în procesele de *machine-learning* care generează, la rândul lor, modele (acele *„inferences”*).

De interes pentru analiza noastră, prin raportare la complexitatea scopului de atins, respectiv posibilitatea algoritmică de a elabora norme juridice, sunt mai degrabă următoarele sisteme: *machine learning* şi *deep learning*.

[9] A. Nordberg, *Trade Secret Protection for AI and Big Data: an oxymoron?*, în J. Schovsbo, T. Minssen, T. Riis (eds.), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive*, Edward Elgar Publishing, 2020, [Online] la https://portal.research.lu.se/portal/files/98797164/Nordberg_Trade_Secrets_Big_data_and_AI_Innovation_version_of_record_before_EE_editing.pdf, accesat 24.11.2021 (traducerea şi interpretarea autorului).

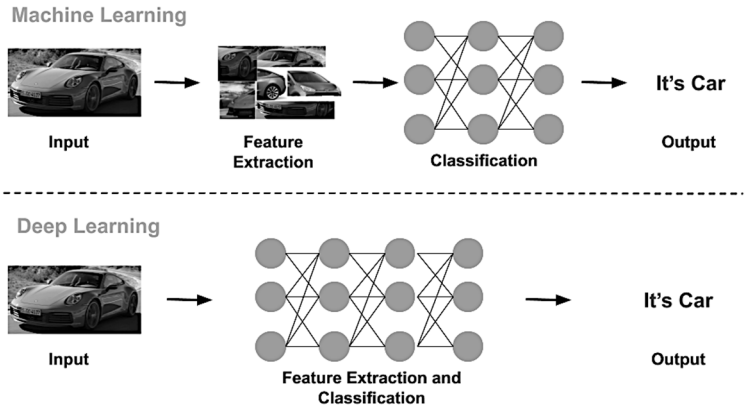

Fig. 2. Pictogramă: *Machine Learning* vs. *Deep Learning*[10]

Machine Learning (ML)	Deep Learning (DL)
Modalitatea concretă este prin metoda „divide et impera", adică se împarte problema complexă în mai multe probleme simple, care se rezolvă separat, iar la final se combină rezultatele pentru a se obține rezultatul final.	Modalitatea concretă este a rezolva problema complexă ducând-o până la capăt (end-to-end), mai întâi prin identificarea tiparelor simple pe baza cărora se pot identifica tiparele complexe.
Sistemul ia decizia singur pe baza experienţelor anterioare din faza de instruire. Regulile în baza cărora va funcționa raționamentul sunt stabilite de către operatorul uman astfel încât decizia (rezultatul final) poate fi uşor de înțeles de către om.	Sistemul ia decizia pe baza rețelelor neuronale artificiale cu multe straturi ascunse, ce imită modalitatea de funcționare a creierului uman, respectiv comunicarea între neuroni prin sinapse. Este o subcategorie a ML care își stabilește singur regulile de raționament astfel încât decizia (rezultatul final) nu poate fi uşor sau chiar deloc de înțeles de către om.
Categoriile de caracteristici distinctive pentru identificarea tiparelor sunt de obicei codate manual de operator (coder), astfel încât faza de instruire durează mai puțin decât faza de testare.	Categoriile de caracteristici distinctive pentru identificarea tiparelor sunt descoperite de către sistem pornind de la cele mai simple până la cele mai complexe, astfel încât faza de instruire durează mai mult decât faza de testare.
Poate fi realizată şi pe computere cu o capacitate de procesare normală.	Poate fi realizată numai pe computere cu o capacitate de procesare foarte mare.
Date puține, dar structurate	Big Data, chiar şi nestructurate
Acuratețe bună, preț scăzut	Acuratețea cea mai bună, prețul foarte mare

Fig. 3. Diferenţe: *Machine Learning* vs. *Deep Learning*[11]

[10] *Machine Learning vs. Deep Learning: What is the Difference*, [Online] la https://www.smlease.com/entries/technology/machine-learning-vs-deep-learning-what-is-the-difference-between-ml-and-dl/, accesat 25.11.2021.

[11] A se vedea D. Garg, S. Khan, M. Alam, *Integrative Use of IoT and Deep Learning for Agricultural Applications*. în P. K. Singh et al. (Eds.): *Proceedings of ICETIT 2019*, LNEE 605, 2020, pp. 521–531, [Online] la https://www.researchgate.net/publication/336000398_Integrative_Use_of_IoT_and_Deep_Learning_for_Agricultural_Applications, accesat 25.11.2021.

Cu cât DL are mai multe straturi ascunse, evident, nivelul de abstractizare a informaţiilor din date creşte, putându-se realiza operaţiuni din ce în ce mai complexe.

Problema care se pune constant este înţelegerea mecanismului de determinare a categoriilor de caracteristici distinctive care se regăseşte în straturi ascunse *(„hidden layers")* şi care conduce la apariţia fenomenului de opacizare, respectiv *„black box"*, în contradicţie cu principiul transparenţei şi al explicabilităţii (din eng. *„explainability"*) ce ar trebui să guverneze orice mecanism cu impact asupra mediului înconjurător, inclusiv asupra drepturilor şi libertăţilor oamenilor. Dacă ar fi să asemănăm cu modul uman de ajungere la un rezultat, cel mai probabil *black box*-ul ar fi o formă de intuiţie umană.

Aşa cum deciziile care pot influenţa drepturile şi libertăţile oamenilor nu se pot baza doar pe intuiţie, mai ales în contextul unor decizii majore, aşa nu este admisibil nici ca un sistem AI să genereze un rezultat al cărui raţionament nu poate fi explicabil.

Cele 4 principii ale explicabilităţii AI sunt:

„(1) *Explanation* (explicare): sistemele furnizează dovezi însoţitoare sau motiv(e) pentru toate rezultatele.

(2) *Meaningful* (sens): sistemele oferă explicaţii care sunt pe înţelesul utilizatorilor individuali.

(3) *Explanation Accuracy* (acurateţea explicaţiei): explicaţia reflectă corect procesul sistemului de generare a rezultatului.

(4) *Knowledge Limits* (limitele cunoaşterii): sistemul funcţionează numai în condiţiile pentru care a fost proiectat sau când sistemul atinge o încredere suficientă în rezultatul său"[12].

Fosca Giannotti, cercetător principal la Institutul de Ştiinţe şi Tehnologie a Informaţiei al Consiliului Naţional de Cercetare din Pisa, Italia, a primit un grant de 2,5 milioane EUR din partea UE pentru a dezvolta până la 30.09.2024 un sistem care să înlăture sau să diminueze problema opacităţii sistemelor AI cu multe straturi ascunse prin determinarea explicaţiilor cauzale, adică tipare care surprind relaţiile cauzale între caracteristici şi decizie, dar şi explicaţii din mecanismul de generare a datelor acestor sisteme complexe[13].

Dacă reunim cele două probleme, respectiv calitatea precară a datelor cu care este alimentat sistemul AI şi opacitatea acestuia, atunci putem asista la un *bias* (subiectivism/ preconcepţie) sistemic, determinat de creşterea exponenţială influenţelor negative asupra rezultatului.

[12] P.J. Phillips, C.A. Hahn, P.C. Fontana, D.A. Broniatowski, M.A. Przybocki, *Four Principles of Explainable Artificial Intelligence*, National Institute of Standards and Technology şi U.S. Department of Commerce August 2020, https://doi.org/10.6028/NIST.IR.8312-draft, accesat 26.11.2021.

[13] A se vedea Proiectul *XAI – Science and technology for the explanation of AI decision making*, [Online] la https://cordis.europa.eu/project/id/834756, accesat 25.11.2021.

2. Posibilitatea normativului algoritmic

Preocuparea de codificare a legislaţiei într-o manieră care să excludă sau să limiteze drastic intervenţia umană a fost dezvoltată de Jeremy Bentham, autorul Raymond Wacks reţinând în legătură cu filosofia lui Bentham următoarele: „Haosul din *common law* trebuia să fie tratat sistematic. Pentru Bentham, aceasta consta, pur şi simplu, în codificare. Codurile juridice ar diminua semnificativ puterea judecătorilor; sarcina lor ar consta mai puţin în interpretarea decât în administrarea legii. De asemenea, ar elimina o mare parte din nevoia de avocaţi: codul ar fi uşor de înţeles fără ajutorul consilierilor juridici"[14]. Chiar dacă Napoleon a realizat codificarea legislaţiei, acest lucru nu a atins perfecţiunea pe care o viza Bentham, ci a fost mai degrabă o activitate de sistematizare.

Filosofia lui Bentham venea în urma ideii matematicianului şi filosofului Gottfried Wilhelm Leibniz, care considera că aplicarea legii nu ar trebui să genereze rezultate contradictorii atâta timp cât legea este interpretată corect. Prin urmare, este nevoie de introducerea unor reguli de interpretare, care, prin aplicarea de către oricine (sau orice, mai nou), să genereze acelaşi rezultat. El avea această concepţie nu numai cu privire la lege, dar o extindea şi la morală, ca factor care generează şi influenţează puternic legea.

René Descartes considera că există „adevărul universal", la care se poate ajunge folosind raţiunea deoarece toate fenomenele sunt explicabile pe deplin atunci când principiile care le guvernează sunt înţelese, acesta fiind motivul pentru care Leibniz considera că mecanismul limbajului şi al cogniţiei pot fi şi ele pe deplin înţelese.

În Călătoriile lui Guliver (1726), autorul Jonathan Swift ironizează ideea lui Leibniz în scena vizitei la Marea Academie din Lagado unde se regăsea „motorul", o maşinărie din lemn cu multe fire pe care sunt mici cuburi de lemn cu simboluri scrise pe fiecare parte. Studenţii Academiei apăsau pe mânerele maşinăriei, determinând cuburile să se rotească şi să afişeze noi combinaţii, după care scriau rezultatul pe o hârtie şi îl înmânau profesorului. În acest fel, profesorul spunea că el şi studenţii pot scrie în mod creativ orice fără cel mai mic ajutor din partea geniului sau a studiului. De fapt, Swift voia să arate că limbajul nu este un sistem formalist care oglindeşte raţionamentul, aşa cum susţinea Leibniz, ci este o formă de exprimare ambiguă care capătă sens doar în contextul folosit, astfel încât este necesar nu doar să ai un set de reguli, ci şi capacitatea necesară de a înţelege adevăratul sens al cuvintelor, contextualizarea[15].

Dreptul Algoritmic este o noţiune umbrelă, care acoperă ansamblul normelor juridice create prin intermediul sistemelor AI, devenind ceea ce am putea

[14] R. Wacks, *Philosophy of Law, A Very Short Introduction,* Ediția a II-a, Editura Oxford University Press, 2014, p. 27.

[15] O. Schwartz, *In the 17th Century, Leibniz Dreamed of a Machine That Could Calculate Ideas The machine would use an "alphabet of human thoughts" and rules to combine* them, 04.11.2019, [Online] la https://spectrum.ieee.org/in-the-17th-century-leibniz-dreamed-of-a-machine-that-could-calculate-ideas, accesat 25.11.2021.

numi ca fiind normativul algoritmic. Acesta poate fi expresia unei sistematizări statistice, a unei prelucrări algoritmice, predictive a situaţiilor din viaţa reală, pe principiul *„if/then"* (trad. „dacă/atunci"), ajungând până la abordări de tipul *Deep Learning*.

Bineînţeles, scopul prelucrărilor de date ar trebui să beneficieze de intervenţie umană, dar setul de date este aproape nelimitat, la fel şi posibilităţile de configurare.

Cel mai simplu mecanism s-ar baza doar pe sistematizare statistică şi un exemplu din viaţa reală ar fi măsurile restrictive din timpul pandemiei care se bazează pe ratele de incidenţă, ale infectărilor precum şi ale deceselor celor afectaţi de pandemia de Covid-19.

Simplist descris, dacă (IF) rata de incidenţă este sub/peste o anumită valoare, atunci (THEN) se iau anumite măsuri restrictive sau nu.

De asemenea, se pot gândi şi sisteme mai complexe, măsurile restrictive care se iau putând fi determinate pe baza statisticilor de focare, dar şi într-o abordare de tipul *Deep Learning*, prin preluarea informaţiilor prelucrate direct din dosarele medicale şi a ratei de incidenţă a contravenţiilor sau infracţiunilor într-un areal.

În acest fel, cantitatea de date şi interpretarea lor ar putea să înlocuiască expunerea de motive/notele de fundamentare ale actelor normative şi, eventual ipoteza normei, iar ulterior, nu omul să fie cel care creează instrucţiunea (dispozitivul şi sancţiunea normei), ci algoritmul însuşi.

Bineînţeles, putem extinde acest exemplu la orice domeniu al dreptului clasic.

Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)[16] (GDPR) prevede în preambul faptul că *persoana vizată ar trebui să aibă dreptul de a nu face obiectul unei decizii, care poate include o măsură, care evaluează aspecte personale referitoare la persoana vizată, care se bazează exclusiv pe prelucrarea automată şi care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă* (pct. 71), dar, conform art. 22 alin. (2) lit. b), dreptul de a nu face obiectul unui proces decizional individual automatizat nu se recunoaşte atunci când decizia *este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului şi care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate.*

Dacă ne referim la situaţia normativului algoritmic, atunci există posibilitatea legală a implementării sale, apreciind totodată că se încadrează în noţiunea de

[16] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), JO L 119, 4.5.2016, p. 1-88, [Online] forma consolidată la 04.05.2016 la https://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504, accesat 25.11.2021.

procese decizionale individuale, chiar dacă norma juridică din sistemul clasic este impersonală.

Prin raportare la art. 6 alin. (2) din Propunerea de Regulament AI, sistemul de inteligenţă artificială care permite conceperea unor norme juridice s-ar putea încadra la sisteme cu grad de risc ridicat. De aceea este necesar să analizăm mai departe riscurile inerente pentru drepturile şi libertăţile fundamentale, precum şi pentru ordinea de drept democratică.

3. Calitatea normativului algoritmic şi riscul sistemic asupra principiilor democratice

Orice schimbare nu trebuie să fie doar posibilă, ci şi să aducă o contribuţie benefică pentru progresul omenirii.

Referindu-ne la legislaţie, deşi există posibilitatea teoretică a creării ei prin intermediul sistemelor AI, aceasta trebuie să asigure respectarea unui principiu esenţial pentru păstrarea încrederii în sistemul normativ şi asigurarea calităţii lui, principiul securităţii juridice. Numai astfel se aduce o contribuţie benefică celor care sunt subiectele ordinii de drept.

Principiul securităţii juridice a fost definit cel mai bine în doctrină ca reprezentând esenţa faptului că oamenii trebuie protejaţi „contra unui pericol care vine chiar din partea dreptului, contra unei insecurităţi pe care a creat-o dreptul sau pe care acesta riscă s-o creeze”[17].

Pe baza sistemului normativ clasic s-a dezvoltat o bogată jurisprudenţă care defineşte condiţiile de calitate ale unei norme, respectiv: accesibilitate, claritate şi previzibilitate.

Pentru ca norma să fie adaptabilă oricăror împrejurări, ea este redactată în termeni generali şi impersonali, fără a depăşi limitele menţionate mai sus, urmând ca cel care o aplică să o interpreteze şi să o raporteze la o situaţie concretă. Am putea descrie această procedură de legiferare ca fiind una de tip *„open box”*, spre deosebire de metoda pe care ar presupune-o utilizarea unui algoritm *(„closed box”)*, o metodă ce ar defini toate situaţiile posibile, le-ar încadra şi le-ar reglementa în detaliu, fără posibilitatea interpretării.

Cu toate acestea, este dificil să ne imaginăm cum ar putea algoritmul să depăşească barierele limbajului natural uman, pe cât de complex, pe atât de frumos, chiar şi în condiţiile în care algoritmii actuali reuşesc să îl proceseze cu acurateţe din ce în ce mai mare, dar doar ca pe o copie fidelă, fără capacitatea de a-i înţelege raţiunile.

[17] L. François, *Le problème de la sécurité juridique, lucrarea La sécurité juridique*, Editura Jeune Barreau de Liège, Liège, 1993, p. 10, *apud.* C.F. Costaş, *Principiul securitatii juridice*, [Online] la https://www.fiscalitatea.ro/principiul-securitatii-juridice-342/, accesat 21.11.2021.

Această orientare a fost descrisă ca pozitivism ştiinţific, „modalitatea carteziană de a privi lumea, într-o cheie strict tehnică, matematică, rece, nu caldă”[18], deşi „spaţiul umanităţii este un spaţiu al fenomenelor, adică al trăirilor, nu al calculelor, al ordonării matematice”[19].

Teoretic ne putem imagina o normă de drept care, în calitate de premisă majoră a silogismului juridic, să epuizeze toate ipotezele care s-ar putea ivi în viaţa reală ca premise minore ale acestuia, permiţând aplicarea legii fără intervenţia omului, ci doar prin recurgere la AI. Întrebarea este cum ar mai putea înţelege subiectul de drept o asemenea normă pentru a se conforma ei? Aceasta ar fi asemenea unei armuri care se mulează perfect pe trupul cavalerului, respectiv pe corpul social, întrucât este construită din foarte multe piese, dar printr-o atare construcţie armura ar deveni atât de grea încât cel ce o îmbracă nu s-ar mai putea mişca, putând fi chiar strivit sub povara ei. Dreptul algoritmic ar fi astfel izvor de securitate, dar o securitate care blochează circuitul juridic şi astfel, progresul. Dintr-o atare perspectivă s-a susţinut că „cu cât dreptul atinge prin fermitatea conceptelor scopul de securitate care îi este propriu, cu atât mai mult riscă să se depărteze de scopul ce-i este comun cu morala: justiţia. O regulă juridică riscă să violeze justiţia cu atât mai puţin cu cât supleţea formulei sale îi permite o mai exactă adaptare la cazul particular; dar atunci ea oferă cu atât mai puţină securitate”[20].

Nevoia inconturnabilă de a realiza echilibrul între drept şi justiţie, între fermitate şi flexibilitate, între previzibil şi imprevizibil, între stabilitate şi dinamism, precum şi între securitate şi progres, a condus la introducerea în ansamblul normativ a „standardelor juridice nedeterminate” care completează înţelesul literal al normei (factor de completare) sau îl corectează (factor de corectare) în funcţie de aprecierea situaţiilor concrete cărora ea ar trebui să i se aplice, şi care acţionează ca „instrument de calificare” a conduitei subiectului de drept sau ca „instrument de diferenţiere” între subiectele de drept şi conduitele acestora. Aceste standarde pătrund în golurile dintre dispoziţiile cu caracter tehnic, astfel încât să îi asigure dreptului vocaţia integratoare pentru întreg universul infinit al raporturilor sociale, asigurând cu fineţe, în situaţii altminteri de neanticipat, ca fiecare să primească ceea ce i se cuvine (*suum cuique tribuere*) şi nimănui să nu i se încalce drepturile (*alterum non laedere*), în acord cu ideea de echilibru ca principiu economic, precum şi ca toţi să trăiască potrivit regulilor binelui şi echitabilului (*honeste vivere*), ca principiu psiho-moral[21]. Dreptul algoritmic nu se poate dispensa de asemenea

[18] G. Colang, *Fundamentele filosofice ale comunicării*, Editura Mustang, Bucureşti, 2018, p. 127, [Online] la http://www.georgecolang.ro/wp-content/uploads/2021/04/George-Colang-Fundamentele-filosofice-ale-comunicarii.-1-Mustang-2018-.pdf, accesat 26.11.2021.

[19] *Ibidem.*

[20] G. Renard, *Le proces du conceptualisme juridique*, în vol. Le Droit, la Logique et le Bon Sens, Paris, 1946, p. 79, *apud.* (citat de) A. Severin, *Elemente fundamentale de drept al comerțului internațional*, Editura Lumina lex, București, 2004, p. 47.

[21] A.M. Naschitz, *Teorie și tehnică în procesul de creare a dreptului*, București, 1969, p. 126, apud. A.Severin, *Elemente fundamentale de drept al comerțului internațional*, Editura

standarde al căror conţinut este determinabil numai în concret şi numai prin evaluarea nuanţată a realităţii din momentul aplicării legii, ceea ce impune recurgerea la inteligenţa umană.

Spre exemplu, conceptul de „bună credinţă" este o valoare juridică fundamentală, care exprimă intima convingere a unei persoane că ceea ce face este bine, în acord nu numai cu legea, dar şi cu morala, sancţionându-se comportamentele abuzive. Fiind legat de o dimensiune intrinsecă fiinţei umane, de o atitudine subiectivă cu privire la un fenomen, acesta nu poate fi copiat. Subiectivismul nu poate fi raţionalizat, el se află în colţul opus obiectivismului.

Dacă ar fi să renunţăm la subiectivism în relaţia cu norma juridică, atunci ar însemna să considerăm că însăşi fiinţa umană este o entitate pur raţională, în schimb, tocmai îmbinarea armonioasă a obiectivismului raţional cu subiectivismul reprezintă semnul distinctiv al chiar formei noastre de inteligenţă, prin comparaţie cu inteligenţa artificială. Conştiinţa umană ne oferă însăşi individualitatea subiectivă, ceea ce stă la baza drepturilor şi libertăţilor noastre fundamentale individuale.

Prin urmare, riscul major identificat se referă la pierderea reperelor individualităţii umane, la reconfigurarea drepturilor şi libertăţilor fundamentale pe care ar urma să le aşezăm pe un pilon colectiv, în desconsiderarea unicităţii fiinţei umane. Ar însemna ca nu algoritmii să înveţe să fie copii fidele ale umanităţii, ci umanitatea să încerce să devină o copie fidelă a algoritmilor, lucru, evident, absurd.

În plus, intervine şi imprecizia retroactivă *(„retroactive vagueness")*, adică nu te poţi raporta la o situaţie cu potenţial în viitorul imprevizibil pentru a-i acoperi în mod categoric şi definitiv toate ipotezele. Nici măcar încercările de construire a tuturor ipotezelor de lucru viitoare pe baza jurisprudenţei, ca sursă de drept, nu poate fi considerată ca acoperind varietatea raporturilor juridice şi modul în care le-am putea interpreta, deşi au existat încercări în acest sens prin construirea sistemului HYPO, ce încerca să modifice situaţiile din cazurile soluţionate în instanţe pentru a testa noi posibilităţi de interpretare a legii, şi apoi CABARET, care se folosea de sistemul anterior pentru un sistem hibrid ce încorpora analiza bazată de jurisprudenţă cu analiza bazată pe raţionamentul juridic[22].

Pe de altă parte, în Cartea Albă privind Inteligenţa artificială – O abordare europeană axată pe excelenţă şi încredere, Comisia Europeană atrage atenţia că inteligenţa artificială „implică o serie de riscuri potenţiale, cum ar fi un proces decizional opac, discriminarea de gen sau de alt tip, intruziunea în viaţa noastră privată sau utilizarea în scopuri infracţionale"[23].

Lumina lex, Bucureşti, 2004, p. 43; A se vedea şi *Buna credinţă*, în I.R. Urs, M. Duţu, A. Severin, S. Angheni, S. Neculaescu (coord.), *Enciclopedia Juridică Română*, vol. I, Editura Academiei Române şi Editura Universul Juridic, Bucureşti, 2018, p. 487 şi urm.

[22] M.A. Livermore, *Rule by Rules*, Computational Legal Studies: The Promise and Challenge of Data-Driven Legal Research (Ryan Whalen, ed.) (2019 Forthcoming), 13 mai 2019, [Online] la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3387701, accesat 26.11.2021.

[23] Comisia Europeană, *Cartea albă privind Inteligenţa artificială - O abordare europeană axată pe excelenţă şi încredere* - COM (2020) 65 final, Comisia Europeană, Bruxelles,

Nu în ultimul rând, trebuie să privim şi la resursele materiale pe care le avem la dispoziţie pentru a realiza un astfel de deziderat, normativul algoritmic. Pentru a putea procesa o cantitate atât de mare de date într-un timp relativ scurt, este nevoie să fie utilizate computerele cuantice, o super-tehnologie destul de nouă şi în continuă dezvoltare, extrem de scumpă şi la care au acces foarte puţini (UE, SUA, China, Germania, Franţa, Marea Britanie, iar dintre privaţi, IBM, Google, Microsoft, Alibaba, Baidu, Tencent[24]).

Acest aspect este tratat pe larg de profesorul Valentin Jeutner în lucrarea sa referitoare la dimensiunile juridice ale computerelor cuantice[25], şi în care introduce imperativul cuantic reflectat în 3 reguli de care atât cei care stabilesc reglementările în domeniu, cât şi cei care dezvoltă computerele cuantice trebuie să ţină seama: (1) acestea să nu creeze sau să exacerbeze inechităţile existente (în special între statele care deţin tehnologia şi cele care nu o deţin); (2) să nu submineze autonomia individuală; (3) să nu se dezvolte soluţii fără a-i consulta pe cei ale căror interese sunt afectate (mai ales în sectorul public, ceea ce înseamnă că inclusiv în ceea ce face obiectul studiului, Dreptul Algoritmic).

Într-o democraţie puterea politică este expresia voinţei poporului, normele juridice fiind o expresie indirectă a voinţei majorităţii. Dar oare însăşi voinţa poporului nu poate fi manipulată printr-o serie de factori astfel încât voinţa reală să fie alterată până la obţinerea unei voinţe contrare celei care ar fi fost obţinută în condiţii normale? Bineînţeles că da, iar dimensiunea istorică ne-a demonstrat acest lucru, mai ales în vremuri în care avem acces la multă informaţie nefiltrată şi suntem presaţi să luăm decizii rapide pe baza acesteia. Astfel, o minoritate cu suficiente resurse materiale poate să influenţeze procesul democratic.

În măsura în care computerele cuantice nu pot fi dezvoltate decât de anumite state sau de privaţi, atunci aceste state sau aceşti privaţi vor deveni forţele dominante la nivel mondial, impunând propriile viziuni asupra lumii, fără capacitatea reală ca ceilalţi participanţi la viaţa democratică să realizeze acest lucru, această tehnologie devenind un instrument foarte util de control al populaţiilor.

În The Great Delusion, autorul John J. Mearsheimer spune că „politica se referă în esenţă la cine poate scrie regulile care guvernează grupul. Această responsabilitate contează foarte mult pentru că membrii oricărei societăţi au sigur nişte interese aflate în conflict, din moment ce nu vor fi niciodată complet de acord cu privire la principiile de bază. Având în vedere acest fapt de bază al vieţii, oricare dintre facţiunile care scrie şi interpretează regulile poate face acest lucru în moduri

19.02.2020, [Online] la https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_ro, accesat 24.11.2021, faţă de care Camera Deputaţilor a României a adoptat opinia exprimată în Hotărârea nr. 28/08.09.2021, publicată în M. Of. nr. 825/09.09.2020.

[24] A se vedea *Who are the main players in the world of quantum computing?*, 16.12.2020, [Online] la https://www.inria.fr/en/quantum-computing-main-players, accesat 25.11.2021.

[25] V. Jeutner, *The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers*, 2021 1(1) Morals & Machines, pp.52-59, ultima revizuire: 18.10.2021 [Online] la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3820003, accesat 25.11.2021.

care să servească interesele sale mai degrabă decât ale rivalilor săi sau să reflecte viziunea sa asupra societăţii, mai degrabă decât a rivalilor săi. Desigur, puterea contează foarte mult pentru a determina ce facţiune câştigă această competiţie. Cu cât un individ sau o facţiune deţine mai multe resurse, cu atât este mai probabil să controleze instituţiile de guvernare. Pe scurt, într-o lume în care raţiunea nu te duce atât de departe, raportul de putere decide de obicei cine trebuie să scrie şi să aplice regulile"[26].

Pe lângă resursele materiale, se mai pun trei probleme.

Una este protejarea acestor super-tehnologii prin brevete de invenţie care fac modificările ulterioare dificil de realizat, deşi ele au încorporate în chiar corpusul lor *bias*-uri în urma faptului că există o mare posibilitate să fie dezvoltate de echipe care nu reflectă diversitatea umană (spre exemplu, diferenţa semnificativă între femei şi bărbaţi care activează domeniul IT). Ca orice creaţie, şi tehnologia însăşi împrumută caracteristicile celui care o dezvoltă, devenind o reflexie fidelă a acestuia. Aceste *bias*-uri devin incorporate în produs şi generează, la rândul lor, alterarea rezultatelor.

A doua este legată de faptul că aceste super-tehnologii nu oferă certitudinea rezultatului astfel încât tot echipa care o dezvoltă este cea care stabileşte marja de eroare, iar aceasta poate fi diferită de la stat la stat, de la stat la privat sau între privaţi. În acest fel, aflându-te sub spectrul aceleiaşi tehnologii, poţi avea diferenţe semnificative în rezultate, lucru care ar trebui reglementat.

GDPR adresează această problemă încă din preambul, statuând faptul că, *pentru a preveni apariţia unui risc major de eludare, protecţia persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic şi să nu depindă de tehnologiile utilizate* (pct. 15).

Ultima problemă se referă la incapacitatea persoanelor, beneficiare ale deciziilor luate de un sistem AI, să le verifice sau să le conteste, ceea ce generează problema lipsei unei răspunderi din cauze obiective.

Acest lucru a fost remarcat şi de alţi autori care spun că „problemele legate de mecanismele de bună guvernare, responsabilitatea şi răspunderea pentru deciziile automate şi statul de drept necesită atenţia legiuitorului în adaptarea prevederilor legale la această nouă formă de luare a deciziilor. Deşi reglementarea generală privind protecţia datelor din Uniunea Europeană este importantă în recunoaşterea procesului decizional automatizat, majoritatea garanţiilor prevăzute de lege în cadrul procesului administrativ echitabil trebuie să fie prevăzute de legiuitorul naţional. Se sugerează că toate ţările trebuie să îşi revizuiască regulile de proces administrativ echitabil în vederea actualizării acestora cu privire la cerinţele procesului decizional automatizat"[27].

[26] J. J. Mearsheimer, *The Great Delusion: Liberal Dreams and International Realities*, Editura Yale University Press, New Haven and London, 2018, p. 21 (traducerea și interpretarea autorului).

[27] M. Suksi, *Administrative due process when using automated decision-making in public administration: some notes from a Finnish perspective*, Artificial Intelligence Law nr. 29/2021,

Toate acestea au fost remarcate în anul 2020 şi de Adunarea Parlamentară a Consiliului Europei, care şi-a manifestat îngrijorările faţă de dezvoltarea şi utilizarea inteligenţei artificiale în procesul democratic în următorii termeni:

„Tehnologiile bazate pe inteligenţa artificială au un impact asupra funcţionării instituţiilor şi proceselor democratice, precum şi asupra comportamentului social şi politic al cetăţenilor. Utilizarea acestora poate produce atât efecte benefice, cât şi dăunătoare asupra democraţiei. Într-adevăr, integrarea rapidă a tehnologiilor AI în instrumentele moderne de comunicare şi platformele de social media oferă oportunităţi unice de influenţă direcţionată, personalizată şi adesea neobservată asupra indivizilor şi grupurilor sociale, pe care diferiţi actori politici pot fi tentaţi să le folosească în propriul beneficiu.

Dintr-o perspectivă pozitivă, IA poate fi folosită pentru a îmbunătăţi responsabilitatea şi transparenţa guvernului, pentru a ajuta la combaterea corupţiei şi pentru a produce multe beneficii pentru acţiunea democratică, participarea şi pluralismul, făcând democraţia mai directă, eficientă şi receptivă la nevoile cetăţenilor. Tehnologiile bazate pe inteligenţa artificială pot lărgi spaţiul pentru reprezentarea democratică prin descentralizarea sistemelor informaţionale şi a platformelor de comunicare. AI poate consolida autonomia informaţională pentru cetăţeni, poate îmbunătăţi modul în care aceştia colectează informaţii despre procesele politice şi îi poate ajuta să participe la aceste procese de la distanţă, facilitând exprimarea politică şi oferind canale de feedback cu actorii politici. De asemenea, poate contribui la stabilirea unei mai mari încrederi între stat şi societate şi între cetăţeni înşişi.

Cu toate acestea, AI poate fi – şi se pare că este – folosită pentru a perturba democraţia prin interferenţa în procesele electorale, *targetarea* personalizată în domeniul politic, modelarea comportamentului alegătorilor şi manipularea opiniei publice. În plus, inteligenţa artificială se pare că a fost folosită pentru a amplifica răspândirea dezinformării, a „camerelor-ecou" (bulelor), a propagandei şi a discursului instigator la ură, erodând astfel gândirea critică, contribuind la creşterea populismului şi la polarizarea societăţilor democratice"[28].

4. Concluzii

Omul nu este şi nu ar trebui vreodată să reprezinte un mijloc, un instrument al tehnologiei, ci un scop în sine. Atâta timp cât nu considerăm că *homo sapiens sapiens* este doar o etapă în evoluţia spre o eră a *homo technologicus* sau chiar a celor care renunţă la orice formă de umanitate, mai avem o şansă să înţelegem că

pp. 87–110, [Online] la https://link.springer.com/article/10.1007/s10506-020-09269-x#citeas, accesat 25.11.2021.

[28] Rezoluția 2341 (2020), *Need for democratic governance of artificial intelligence*, Adunarea Parlamentară a Consiliului Europei, 22.10.2020, [Online] la https://pace.coe.int/pdf/0b472b0ef9de710970a8106e0bbaf0d10fe3b0119e48da83a286ab652d6e66b9/resolution%202341.pdf, accesat 24.11.2021 (traducerea și interpretarea autorului).

ceea ce ne face umani, expresia fragilităţii noastre, nu este o vulnerabilitate, ci o super-putere.

În acord cu această concepţie este şi modalitatea în care înţelegem să reglementăm raporturile sociale sub aspect juridic între actorii umanităţii, apelând la instrumente specifice care trimit la conştiinţă, la moralitate, şi îndepărtându-ne de ceea ce este calculat, matematic, rece.

Prin urmare, chiar dacă, din punct de vedere tehnic, Dreptul Algoritmic ne oferă facilităţi în ceea priveşte redactarea, interpretarea şi aplicarea normelor de drept, oferta pe care ne-o face trebuie acceptată cu rezerve şi consumată *cum granum salis*, căci, altminteri, ea nu este decât un fruct otrăvit întrucât rescrie paradigma omului care utilizează instrumentul, transformând omul însuşi într-un instrument aruncat în capcana tehnologiei.

Referinţe

Aristotel, *Politica*, Năstase N. (red.), ediţie actualizată a lucrării *Politica* apărută la editura Cultura Naţională în anul 1924, traducere de El. Bezdechi, Editura Biblioteca Centrală Universitara „Lucian Blaga"

Bostrom N., *Superinteligenţa. Direcţii, pericole, strategii*, Editura Litera, Bucureşti, 2019

Brockman J., *Minţi posibile: douăzeci şi cinci de perspective asupra inteligenţei aritificiale*, Editura Vellant, Bucureşti, 2019

Colang G., *Fundamentele filosofice ale comunicării*, Editura Mustang, Bucureşti, 2018

Coleman F., *A Human Algorithm: How Artificial Intelligence is Redefining Who We Are*, Editura Counterpoint, Berkeley, California, 2019

Comisia Europeană, Directoratul General pentru Comunicare, High-Level Expert Group on Artificial Intelligence, *A definition of AI: Main capabilities and scientific disciplines*, Comisia Europeană, B-1049 Bruxelles

Comisia Europeană, *Cartea albă privind Inteligența artificială - O abordare europeană axată pe excelență şi încredere* (Cartea Albă COM(2020) 65 final), Comisia Europeană, Bruxelles, 2020

Costaş C.F., *Principiul securităţii juridice*, [Online]

Craglia M. (Ed.), Annoni A., Benczur P. Bertoldi P., Delipetrev P., De Prato G., Feijoo C., Fernandez M.E., Gomez E., Iglesias M., Junklewitz H., López Cobo M., Marténs B., Nascimento S., Nativi S., Polvora A., Sanchez I., Tolan S., Tuomi I., Vesnic Alujevic L., *Artificial Intelligence - A European Perspective*, EUR 29425 EN, Publications Office, Luxembourg, 2018, https://doi.org/10.2760/11251

Devecka M., *Did the Greeks Believe in their Robots?* în The Cambridge Classical Journal, 59, 2013, https://doi.org/10.1017/S1750270513000079

Garg, D., Khan S., Alam M., *Integrative Use of IoT and Deep Learning for Agricultural Applications*, în P. K. Singh et al. (Eds.): *Proceedings of ICETIT 2019*, LNEE 605, 2020, http://dx.doi.org/10.1007/978-3-030-30577-2_46

Jeutner V., *The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers* vol. 1 (1) Morals & Machines, 2021

Kaplan J., *Artificial Intelligence. What Everybody Needs to Know*, Editura Oxford University Press, Marea Britanie, 2016

Krimmel J., *Artificial Intelligence Started with the Calendar and Abacus*, 2017

Kumar P., *Artificial Intelligence: Reshaping Life and Business*, Editura BPB Publications, New Delhi, 2019

Livermore M.A., *Rule by Rules*, Computational Legal Studies: The Promise and Challenge of Data-Driven Legal Research (Ryan Whalen, ed.), 2019, https://doi.org/10.2139/ssrn.3387701

Mearsheimer J.J., *The Great Delusion: Liberal Dreams and International Realities*, Yale University Press, New Haven, 2018

Mitchell M., *Artificial intelligence : a guide for thinking humans*, Editura Farrar, Straus and Giroux, New York, 2019

Nordberg A., *Trade Secret Protection for AI and Big Data: an oxymoron?*, în Schovsbo J., Minssen T., Riis T. (eds.), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive*, Edward Elgar Publishing, 2020

Phillips P.J., Hahn C.A., Fontana P.C., Broniatowski D.A., Przybocki M.A., *Four Principles of Explainable Artificial Intelligence*, National Institute of Standards and Technology şi U.S. Department of Commerce August 2020

Pickover C.A., *Artificial Intelligence – An Illustrated History, From Medieval Robots to Neural Networks*, Editura Sterling Publishing Co., Inc, New York, 2019, ISBN: 978-1-4549-3359-5

Schwartz O., *In the 17th Century, Leibniz Dreamed of a Machine That Could Calculate Ideas The machine would use an „alphabet of human thoughts" and rules to combine* them, 2019

Severin A., *Elemente fundamentale de drept al comerţului internaţional*, Editura Lumina lex, Bucureşti, 2004

Stănilă L.M., *Inteligenţa artificială, dreptul penal şi sistemul de justiţie penală: amintiri despre viitor*, Editura Universul Juridic, Bucureşti, 2020

Tegmark M., *Viaţa 3.0: Omul în epoca inteligenţei artificiale*, Editura Humanitas, Bucureşti, 2019

Suksi M., *Administrative due process when using automated decision-making in public administration: some notes from a Finnish perspective.* Artificial Intelligence Law 29, 87–110 (2021), https://doi.org/10.1007/s10506-020-09269-x

Susskind J., *Politica viitorului. Tehnologia digitală şi societatea*, Editura Corint Future, Bucureşti, 2019

Urs I.R., Duţu M., Severin A., Angheni S., Neculaescu S. (coord.), *Enciclopedia Juridică Română*, vol. I, Editura Academiei Române şi Editura Universul Juridic, Bucureşti, 2018

Yeung K., Lodge M., *Algorithmic Regulation*, Editura Oxford University Press, 2019, ISBN 978-0-19-883849-4

Wacks R., *Philosophy of Law, A Very Short Introduction*, Ediţia a II-a, Editura Oxford University Press, Marea Britanie, 2014

Webb A., *Cei nouă titani tech. Cum va schimba inteligenţa aritificială cursul omenirii*, Editura Globo, Bucureşti, 2019

Wilks Y, *Artificial Intelligence: Modern Magic or Dangerous Future?*, Editura Icon Books Ltd., 2019

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-24

Natura şi impozitarea veniturilor realizate din activitatea de *streaming*

The Nature and Taxation of Income from Streaming Activity

Marius-Cosmin Macovei[1], **Rareş-Vasile Voroneanu-Popa**[2]

Rezumat: Prezenta lucrare propune relevarea unor aspecte de drept fiscal privind natura şi modul de impozitare a veniturilor realizate de persoanele fizice care pun la dispoziţia consumatorilor conţinut digital, în urma încheierii cu aceştia din urmă a unui contract de furnizare de conţinut digital, pe scurt, activitatea de *streaming*. Cu toate că acest concept a apărut de acum aproape o sută de ani, *streaming*-ul a devenit un instrument des utilizat după anii 2000 în industria jocurilor video, muzică, televiziune şi radio. În ultimii ani însă, cu precădere în anul 2020, a devenit o sursă importantă de venit pentru diverse categorii de persoane, activă pentru unele, ajungând să fie un loc de muncă, sau pasivă, ca hobby. Creşterea considerabilă a acestora, implicit şi a cuantumului veniturilor realizate poate însă ridica probleme, precum dacă şi în ce mod pot fi impozitate, date fiind formele de obţinere a lor.

Cuvinte-cheie: streaming; drept fiscal; impozit; venituri; contract

Abstract: This paper proposes to reveal some aspects of tax law regarding the nature and method of income taxation made by individuals who provide consumers with digital content, following the conclusion with the latter of a contract for the supply of digital content, in short, the activity of streaming. Although this concept appeared almost a hundred years ago, streaming has become a tool often used since the late 2000s in the video game, music, television and radio industries. In recent years, however, especially in 2020, it has become an important source of income for various categories of people, active for some, becoming a job, or passive, as a hobby. However, the considerable increase of them, implicitly and of the amount of realized incomes can raise problems, as well as if and in what way they can be taxed, given the forms of obtaining them.

Keywords: streaming; tax law; tax; income; contract

[1] Consilier juridic, Asociația Profesională Colegiul Consilierilor Juridici din Iași, e-mail: mariuscosminmacovei@gmail.com.

[2] Asistent univ. drd., Universitatea „Grigore T. Popa” din Iași, e-mail: raresvoroneanu95@gmail.com.

1. Introducere

Tehnologia a evoluat considerabil în ultimii ani, devenind un element indispensabil pentru ceea ce oamenii întreprind zilnic în viaţa lor. Pandemia provocată de virusul Sars-Cov-2 a ţinut persoanele la distanţă şi le-a demonstrat că în continuare este nevoie de tehnologie în orice activitate desfăşurată, de la interacţiune socială, divertisment, şi până la prestarea muncii.

În ultimii ani au apărut multiple oportunităţi de învăţare şi dezvoltare în mediul online, oferite de persoane cu experienţă în diverse domenii, activităţi care pot fi generatoare de venituri. Acest fapt a fost îmbucurător pentru participanţii la circuitul civil cărora circumstanţele actuale le ofereau incertitudine în privinţa situaţiei financiare. Astfel, aceştia au descoperit că pot transforma propriile activităţi alocate timpului liber în mijloace care să devină o sursă de venit. Realizarea unor venituri destul de consistente generează şi interogaţii, precum dacă există obligaţia de a declara veniturile, de a plăti impozit şi în ce cota.

În context mai larg, Constituţia conferă oricărei persoane fizice libertatea de a desfăşura, în condiţiile legii, o activitate economică, din proprie iniţiativă, fără a fi necesară ca aceasta să dobândească o calitate formală sau o autorizare specială ori în baza calităţilor personale sau a pregătirii sale profesionale[3].

2. Definirea activităţii de streaming

Activităţile de *streaming* reprezintă consumul de conţinut digital fără stocarea locală, respectiv descărcarea pe un dispozitiv al consumatorului de materiale video şi/sau audio preînregistrate, transmisii în direct (conferinţe, emisiuni tv, radio, jocuri). Exemple bine-cunoscute în acest sens sunt YouTube, Netflix, HBOGo, Spotify, Apple Music, Twitch etc.

Accesul la serviciile de *streaming* are loc prin încheierea unei convenţii între furnizori şi consumatori, aceasta având natura unui contract, de regulă, în format digital, în baza condiţiilor platformei. Nu este necesară întâlnirea fizică dintre părţi, furnizorul punând la dispoziţia consumatorilor un contract prestabilit, cu toate informaţiile despre serviciile oferite, preţurile acestora, termenii şi condiţiile de prestare, în timp ce consumatorii oferă o serie de date personale pentru a primi serviciile dorite[4].

Convenţia ia forma unui abonament cu plata lunară/ trimestrială/ anuală, oferit de furnizor contra unei sume ce poate fi debitată direct de pe cardul consumatorului, înregistrat în contul creat pe platformă.

Din punct de vedere comercial, activitatea de *streaming* este realizată conform codului 6311, prevăzut de Clasificarea Activităţilor din Economia

[3] C. Ionescu, C.A. Dumitrescu, (coordonatori), C. Bălăceanu, T. Corlăţean, C. Jora, L. Macarovschi, B. Pătraşcu, A.M. Popescu, R. Popescu, D.M. Tilea, *Constituția României. Comentarii și explicații*, Editura C. H. Beck, Bucureşti, 2017, p. 555.

[4] [Online] la https://support.google.com/youtube/answer/9961934?hl=en, accesat 26.11.2021.

Naţională, conform căruia agenţii economici[5] (organizaţi conform Legii nr. 31/1990 privind societăţile sau O.U.G. nr. 44/2008 privind desfăşurarea activităţilor economice de către persoanele fizice autorizate, întreprinderile individuale şi întreprinderile familiale) prestează activităţi de prelucrare a datelor, administrarea paginilor web şi activităţi conexe, în care sunt incluse şi servicii de *streaming* („organizare de fluxuri").

Majoritatea platformelor menţionate anterior, care obţin venituri din *streaming*, sunt deţinute de companii internaţionale, direct sau prin interpuşi ai acestora, astfel că acestea plătesc impozite aferente veniturilor societăţilor în funcţie de statul în care sunt înregistrate. În România, aceste impuneri pot fi de natura impozitului pe profit sau a impozitului pe veniturile microîntreprinderilor (pentru persoanele juridice) şi a taxei pe valoarea adăugată (atât pentru persoanele juridice, cât şi pentru persoanele fizice).

3. Activităţi prevăzute de legislaţia fiscală

Codul Fiscal prevede în cazul persoanelor fizice o serie de venituri ce pot fi impozitate, precum şi unele care sunt scutite de impozit.

Pentru ca veniturile să fie impozabile, activitatea desfăşurată trebuie să constituie un fapt juridic generator al impunerii, respectiv „evenimentul indicat de lege, care se produce în patrimoniul unei persoane şi determină apariţia de obligaţii fiscale patrimoniale"[6].

Se disting astfel următoarele fapte juridice: a) realizarea unui venit/profit/ câştig – sursa venitului poate fi una din următoarele: un act juridic cu titlu oneros (contract de vânzare, contract de muncă, contract de închiriere etc.); activitate profesională (activitate economică, în cazul persoanelor juridice, sau activitate independentă - profesie liberală, proprietate intelectuală, în cazul persoanelor fizice) sau alte surse. b) efectuarea unui act juridic cu privire la un bun sau un serviciu (act economic sau act de consum), respectiv efectuarea de către o persoană impozabilă sau un consumator a unei achiziţii de bunuri sau servicii. c) deţinerea în proprietate a unui bun, care implică şi o serie de obligaţii patrimoniale în sarcina proprietarului, sub formă de impozite şi taxe, ca accesorii ale dreptului de proprietate asupra bunului[7].

Dintre cele trei fapte juridice, considerăm că activitatea de *streaming* poate fi caracterizată ca fiind de natura realizării unui venit ce are ca sursă o activitate desfăşurată de o persoană juridică, ca activitate comercială, sau de o persoană fizică, ca activitate independentă, exploatare a drepturilor de proprietate intelectuală sau altă categorie de activitate (din care se obţin venituri din categoria „alte surse").

[5] [Online] la https://www.onrc.ro/index.php/ro/caen, accesat 26.11.2021.

[6] I.M. Costea, *Fiscalitate europeană. Note de curs,* Editura Hamangiu, Bucureşti, 2016, p. 5.

[7] *Idem,* p. 6-7.

În ceea ce priveşte persoanele fizice, am identificat trei categorii în care pot fi incluse veniturile realizate de persoanele fizice din activitatea de *streaming*, pe care le vom trata în cele ce urmează.

O primă categorie de clasificare a acestor venituri ar fi ca venituri provenite din activităţi independente – exercitarea acestora cu regularitate, pe cont propriu şi în realizarea unui scop lucrativ[8]. Raportat la dispoziţiile Codului Fiscal, respectiv la cele privind definirea activităţii independente, activitatea de *streaming* pe care o efectuează persoanele fizice poate fi inclusă în această categorie, întrucât întruneşte cel puţin 4 criterii dintre cele enumerate, deşi nu este şi o activitate ce poate fi regăsită în Clasificarea Ocupaţiilor din România.

În categoria veniturilor provenite din activităţile prestate în mod independent sunt incluse veniturile profesionale (comerţ, prestări servicii, meserii) şi veniturile din exercitarea profesiilor liberale.

Profesiile liberale sunt definite ca fiind activităţile cu caracter intelectual, ce solicită un nivel înalt de calificare şi sunt de regulă reglementate strict de regulamente/statute exacte şi clare[9]. Dat fiind faptul că persoanele care realizează activităţi de *streaming* nu probează elementele definitorii enunţate anterior, apreciem că aceasta nu poate reprezenta o profesie liberală.

În ansamblu, desfăşurarea unei activităţi independente trebuie să îndeplinească două condiţii, respectiv: a) activitatea să fie din ariile următoare: producţie, comerţ, prestări de servicii sau profesii liberale; b) activitatea desfăşurată să îndeplinească cel puţin patru dintre următoarele şapte criterii prevăzute de art. 7 pct. 3 din Codul Fiscal: 1) libertatea conferită persoanei fizice de a-şi alege locul, programul şi modalitatea de exercitare a activităţii; 2) posibilitatea de a exercita activitatea pentru mai mulţi clienţi; 3) asumarea de către persoana ce desfăşoară activitatea a eventualelor riscuri ce se pot ivi; 4) realizarea activităţii prin utilizarea patrimoniului persoanei fizice care o desfăşoară; 5) persoana fizică ce exercită activitatea utilizează capacitatea intelectuală şi/sau a prestaţiei fizice a acesteia, ce depinde şi de specificul activităţii; 6) persoana fizică este membru al unei forme de organizare profesională ce are rolul de reprezentare, reglemente şi supraveghere a profesiei exercitate, în conformitate cu actele normative speciale ce reglementează organizarea şi exercitarea profesiei; 7) libertatea persoanei fizice de a desfăşura activitatea în mod direct, cu personal angajat sau în colaborare cu persoane terţe în condiţiile legii[10].

În sinteză, caracterul independent al unei activităţi poate fi luat în considerare atunci când: 1) activitatea pe care o exercită o persoană care nu este organic inclusă într-o organizaţie, privată sau publică; 2) persoana care desfăşoară activitatea are libertatea de a se organiza corespunzător, în ceea ce priveşte

[8] I.M. Costea, *Drept financiar,* Ediția a 7-a, revăzută și adăugită, Editura Hamangiu, București, 2021, p. 205.

[9] *Ibidem.*

[10] M. Ene, *Drept fiscal. Curs introductiv,* Editura Solomon, București, 2020, p. 106-107.

resursele umane şi materiale folosite în realizarea activităţii; 3) persoana în cauză suportă eventualul risc economic al activităţii[11].

Printre criteriile care definesc preponderent existenţa unei activităţi independente sunt: libera alegere a desfăşurării activităţii, a programului de lucru şi a locului de desfăşurare a activităţii; riscul pe care şi-l asumă întreprinzătorul; activitatea se desfăşoară pentru mai mulţi clienţi; activitatea se poate desfăşura nu numai direct, ci şi cu personalul angajat de întreprinzător în condiţiile legii.

Pe lângă includerea în categoria veniturilor din activităţi independente, va trebui analizată şi modalitatea în care se determină venitul net asupra căruia se va aplica cota de impunere. Acest fapt va implica evidenţierea veniturilor, dar şi a cheltuielilor deductibile, integral şi limitat, pe care le realizează aceste persoane, precum şi a cheltuielilor nedeductibile. Cota de impunere a acestui tip de venituri, prevăzută de Codul Fiscal, este de 10% din veniturile nete realizate.

Cea de-a doua categorie în care se pot încadra veniturile obţinute din activitatea de *streaming* este cea a veniturilor provenite din drepturi de proprietate intelectuală, în conformitate cu art. 70 din Codul Fiscal, coroborat cu dispoziţiile art. 7 şi 65 din Legea nr. 8/1996 privind drepturile de autor şi drepturile conexe, republicată[12].

În interpretarea textelor de lege enunţate, veniturile din activitatea de *streaming* pot fi incluse în această categorie datorită legăturii dintre sintagma *„şi alte asemenea”* din cuprinsul art. 70 cu sintagma *„orice alte opere audiovizuale”* din cuprinsul art. 7 lit. e) din Legea nr. 8/1996, a cărei definiţie se regăseşte la art. 65 din acelaşi act normativ: *„Opera audiovizuală este opera cinematografică exprimată printr-un procedeu similar cinematografiei sau orice altă operă constând dintr-o succesiune de imagini în mişcare, însoţite sau nu de sunete”.*

În această ipoteză, venitul net se determină prin deducerea din venituri a cheltuielilor efectuate, determinate prin aplicarea asupra veniturilor brute a cotei forfetare de 40%. Cota de impunere aplicată venitului net rezultat este de 10%.

Finalmente, a treia categorie de venituri în care se pot încadra veniturile realizate de persoanele fizice din activitatea de *streaming* este cea a veniturilor neimpozabile, respectiv sumele de bani primite cu titlu de donaţie, prevăzute de art. 62 Cod Fiscal. Aşadar, conform legislaţiei fiscale din România, pentru veniturile obţinute din donaţii, nu se datorează impozit.

Din punct de vedere juridic, astfel de donaţii nu trebuie încheiate prin înscris autentic, conform prevederilor art. 1011 Cod Civil. De asemenea, nu ne aflăm în prezenţa unei donaţii deghizate, întrucât, de regulă, voinţa reală a părţilor nu este ascunsă. În aceste condiţii, actul juridic respectiv poate reprezenta fie un dar manual, dat fiind faptul că reprezintă un acord de voinţă dintre donator şi donatar şi predarea efectivă a banilor are loc instantaneu, însă până la limita de 25.000 de lei, fie o donaţie indirectă, fiind un act de gratificare care produce efecte juridice ca

[11] C.F. Costaș, *Drept fiscal,* Editura Universul Juridic, București, 2021, p. 205, Opinia avocatului general Tesauro în cauza C-202/90, *Ayuntamiento de Sevilla c. Recaudadores de Tributos de las Zonasprimera y segunda,* în *Culegere 1991,* pp I-4247.

[12] Publicată în M. Of. nr. 489 din 14 iunie 2018.

ale donaţiei[13]. Totodată, acestea nu pot fi considerate acte de sponsorizare, întrucât nu au forma unui contract negociat care să stipuleze obiectul, valoarea şi durata sponsorizării, nici acte de mecenat, activitatea de *streaming* nefiind inclusă, la acest moment, în una dintre categoriile artistic, cultural, medico-sanitar sau ştiinţific (cercetare fundamentală şi aplicată)[14].

Donaţia este des întâlnită pe canalele de *streaming* ale persoanelor fizice, cei care le urmăresc fiind încurajaţi să susţină activitatea persoanei prin astfel de acte cu titlu gratuit.

În cazul unui canal de YouTube, donaţiile se pot efectua fie în timpul sesiunilor *live*, prin *superchat*[15], fie în afara acestor sesiuni. Ca metodă de plată, se foloseşte, de regulă, sistemul de conturi PayPal[16].

În cazul platformei Twitch, se utilizează *bits*, care reprezintă sistemul oficial de donare al acestui canal. *Bits* îmbracă o formă digitală şi pot fi obţinuţi prin achiziţionarea directă de pe platforma Twitch, utilizând monedă fiduciară, prin intermediul Amazon Payments. În cadrul acestei platforme se pot utiliza şi donaţiile prin PayPal, ca metodă mai uşoară comparativ cu cea prin *bits*, banii fiind transmişi direct, prin intermediul adresei de email asociate contului de PayPal al consumatorului de conţinut.

Veniturile realizate de o persoană pe această platformă ajung, în medie, la valori de cel puţin 3.000 până la 5.000 de dolari pe lună, pentru o activitate de 40 de ore pe săptămână.

4. Concluzii

Activitatea de *streaming* a persoanelor fizice poate reprezenta o sursă semnificativă de venituri la bugetul de stat, iar o reglementare viitoare suplimentară, în sensul includerii în Clasificarea Ocupaţiilor din România, ar putea fi de asemenea binevenită.

În ceea ce priveşte mijlocul de control al obţinerii veniturilor, acesta este deja parţial creat, majoritatea sumelor fiind primite în conturile bancare ale beneficiarilor.

Dincolo de faptul că cei care desfăşoară astfel de activităţi au deja o motivaţie personală în acest sens, reglementarea expresă ar deveni, probabil, benefică şi

[13] I. Nicolae, *Varietăți de donații și particularitățile acestora,* [Online] la http://revista.universuljuridic.ro/varietati-de-donatii-si-particularitatile-acestora-2/, accesat 27.11.2021.

[14] S. Mitu, *Despre Sponsorizare, Donaţie şi Mecenat, sau cum pot acorda firmele ajutor în pandemie şi nu numai*, [Online] la https://www.zf.ro/opinii/despre-sponsorizare-donatie-si-mecenat-sau-cum-pot-acorda-firmele-19776341, accesat 27.11.2021.

[15] *"Super Chat and Super Stickers are ways to monetise your channel through the YouTube Partner Programme. These features let your viewers purchase chat messages that stand out and sometimes pin them to the top of a chat feed."*, [Online] la https:// support.google.com/ youtube/answer/7288782?hl=en-GB, accesat 27.11.2021.

[16] [Online] la https://support.google.com/youtube/answer/6319255?hl=en#:~:text=Make%20sure%20you've%20set,in%20the%20chat%20on%20mobile, accesat 27.11.2021.

pentru aceştia. Totodată, trebuie ţinut cont şi de faptul că, aşa cum se doreşte şi în cadrul altor activităţi care generează venituri, şi în acest caz este nevoie de crearea unui cadru legal cât mai puţin birocratic şi încărcat din punct de vedere fiscal.

Referinţe

Costea, I.M., *Drept financiar*, ediţia a 7-a, revăzută şi adăugită, Editura Hamangiu, Bucureşti, 2021

Costea, I.M., *Fiscalitate europeană*, Editura Hamangiu, Bucureşti, 2016

Costaş, C.F., *Drept fiscal*, Editura Universul Juridic, Bucureşti, 2021

Ene, M., *Drept fiscal*, Editura Solomon, Bucureşti, 2021

Ionescu, C., Dumitrescu, C.A. (coordonatori), Bălăceanu, C., Corlăţean, T., Jora, C., Macarovschi, L., Pătraşcu, B., Popescu, A.M., Popescu, R., Tilea, D.M., *Constituţia României. Comentarii şi explicaţii*, Editura C. H. Beck, Bucureşti, 2017

Mitu S., *Despre Sponsorizare, Donaţie şi Mecenat, sau cum pot acorda firmele ajutor în pandemie şi nu numai*, [Online]

Nicolae I., *Varietăţi de donaţii şi particularităţile acestora*, [Online]

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

DOI: 10.47743/jss-2021-67-4-25

Aspecte de drept comparat privind metodele speciale de supraveghere sau cercetare utilizate în lupta împotriva criminalităţii informatice în legislaţia din România şi Republica Moldova

Aspects of Comparative Law Regarding the Special Methods of Surveillance or Research Used in the Fight Against Computer Crime in the Legislation of Romania and the Republic of Moldova

Vasile Popa[1]

Rezumat: În ultimii ani, favorizată şi de situaţia pandemică, s-a observat că în timp ce lumea digitală aduce beneficii enorme, creează şi mari vulnerabilităţi. Incidentele din spaţiul virtual sunt în creştere la un nivel alarmant şi ar putea perturba furnizarea de servicii esenţiale, prin ameninţări cu origini diferite, îndreptate atât asupra persoanelor fizice cât şi juridice. Internetul, ca instrument principal al criminalităţii informatice, prezinta o infinitate de utilizări, ceea ce duce în mod inevitabil la diversificarea formelor de manifestare a fenomenului. Menţinerea unei siguranţe în mediul informatic a devenit o prioritate a securităţii tuturor statelor, care potrivit convenţiilor şi tratatelor internaţionale se poate realiza prin, cunoaşterea, prevenirea şi contracararea atacurilor şi ameninţărilor, precum şi prin diminuarea vulnerabilităţilor infrastructurilor cibernetice în scopul gestionării eficiente a tuturor riscurilor la adresa securităţii acestora, prevenirea şi combaterea criminalităţii informatice şi nu în ultimul rând apărarea cibernetică. Contribuţia în săvârşirea faptelor penale a mijloacelor informatice, au motivat reglementarea unor procedee probatorii speciale, adaptate la lumea în care trăim, a căror utilizare facilitează procesul de tragere la răspundere penală a persoanelor care comit infracţiuni.

Cuvinte-cheie: procedee probatorii; criminalitate informatică; măsuri speciale de supraveghere; proces penal

Abstract: In recent years, also favored by the pandemic situation, it has been observed that while the digital world brings enormous benefits, it also creates great vulnerabilities. Incidents in the virtual space are growing at an alarming level and could disrupt the provision of essential services, through threats with different origins, aimed at both individuals and legal entities. The Internet, as the main tool of cybercrime, has an infinite number of uses, which inevitably leads to the diversification of the manifestations of the phenomenon. Maintaining security in the IT environment has become a priority for the

[1] Doctorand, Universitatea de Stat din Moldova, Școala Doctorală Științe Juridice, e-mail: sile_popa18@yahoo.com.

security of all states, which according to international conventions and treaties can be achieved by knowing, preventing and countering attacks and threats, as well as by reducing the vulnerabilities of cyber infrastructures in order to effectively manage all risks. addressing their security, preventing and combating cybercrime and last but not least cyber defense. The contribution in committing the criminal acts to the computer means, motivated the regulation of special evidentiary procedures, adapted to the world in which we live, whose use facilitates the process of prosecuting the persons who commit crimes.

Keywords: evidentiary procedures; cybercrime; special surveillance measures; criminal proceedings

Dezvoltarea fulminantă a tehnologiei a creat, pe lângă numeroase beneficii, şi situaţii mai puţin plăcute; putem spune că a deschis adevărate oportunităţi pentru încălcări greu de detectat şi combătut şi care produc permanent prejudicii însemnate.

August Beguai menţiona într-un studiu că, în timp ce în 1984 al lui Orwell oamenii se aflau sub ochiul Marelui Frate şi al Poliţiei Secrete a acestuia, astăzi se află sub ochiul marilor sisteme informatizate. Fără lege şi ordine în această societate informatizată declinul va fi în mod cert provocat chiar de aceste cuceriri tehnologice care pe de altă parte aduc atâtea beneficii omenirii.

Despre sistemul judiciar din Republica Moldova, de după anul 1991 s-a afirmat că reformarea a fost realizată pe cale evoluţionară şi nu revoluţionară, sistemul anterior constituind baza noii puteri judiciare, cu toate că legile noi au instituit noi raporturi şi organisme statale în sistemul judiciar. Vechiul sistem legislativ, oricâte completări, modificări sau abrogări de texte ar suporta, rămâne expresia unei anumite perioade istorice, astfel subliniază că noul sistem de justiţie nu poate apărea din nimic ori în baza inspiraţiei iniţiatorilor sau cu fragmente de idei selectate aleatoriu din experienţa altor state, ci doar având la bază o seamă de obiceiuri, tradiţii şi precedente, scopul fiind afirmarea şi consolidarea statului de drept şi al edificiului democratic privind înfăptuirea justiţiei[2].

Necesitatea reglementării prin norme juridice a domeniului delicat al activităţii speciale de investigaţii s-a materializat iniţial prin Legea nr. 45/1994[3], ca regim extrajudiciar de activităţi şi investigaţii operative, asociate vechilor coduri penale şi de procedură penală şi care în mod generic, a fost definită ca fiind „primul act normativ ce reglementează deschis activitatea secretă a serviciilor speciale şi în care au fost concentrate şi unificate reguli de bază privind activitatea cotidiană,

[2] T. Osoianu, *Reforma judiciară şi de drept în Republica Moldova. Condiție necesară în vederea integrării europene*, [Online] la http: //www.ipp.md/old/print.php?l=ro&idc=167& id=495, p. 1-2, 15 şi Apud din Мартынчик Е., *Судебная власть в Молдове*, часть первая (историко-правовые очерки), Изд-во ULIM, Chișinău, 1999, p. 23, accesat 31.03.2019.

[3] Legea nr. 45/12.04.1994 privind activitatea operativă de investigații (A.S.I.), publicată în Monitorul Oficial al Republicii Moldova nr. 11-13/1994, abrogată prin Legea nr. 59/29.03.2012, accesat 31.03.2019.

fără excepţii, a organelor investite cu dreptul de a efectua activitatea operativă de investigaţii”[4].

Conform Legii nr. 45/1994, activitatea operativă de investigaţii, constituie un mijloc juridic de stat, de apărare a intereselor statului, integrităţii teritoriale, drepturilor şi intereselor legitime ale persoanelor, a tuturor formelor de proprietate contra atentatelor criminale, cu *sarcini* de: relevarea atentatelor criminale, prevenirea, curmarea, descoperirea infracţiunilor şi a persoanelor care le organizează, le comit sau le-au comis, precum şi compensării daunei cauzate de infracţiune; căutarea persoanelor care se ascund de organele de urmărire penală sau de judecată sau care se sustrag de la sancţiunea penală şi a celor dispăruţi fără urmă; colectarea de informaţii despre evenimentele sau acţiunile care pun în pericol securitatea de stat, militară, economică sau ecologică a ţării, desfăşurată în baza principiilor legalităţii, respectării drepturilor omului şi libertăţilor persoanei, oportunităţii şi ofensivităţii, îmbinării metodelor publice şi secrete, cooperării cu alte organe de stat, dez-ideologizării şi nepărtinirii.

Normele nepublice, conspirate sunt condiţionate a se aplica numai în cazul în care este imposibilă o altă cale, în scopul îndeplinirii sarcinilor activităţii operative de investigaţii necesare pentru asigurarea securităţii naţionale, ordinii publice, bunăstării economice, menţinerii ordinii de drept şi prevenirea sau descoperirea infracţiunilor grave, deosebit de grave şi excepţional de grave, pentru ocrotirea sănătăţii, protejarea moralităţii ori pentru apărarea drepturilor şi libertăţilor altor persoane.

Activităţile concrete conform articolului 6 din Legea nr. 45/1994 sunt distribuite a se realiza, astfel: cu autorizarea judecătorului de instrucţie (cercetarea domiciliului şi instalarea în el a aparatelor audio, video, de fotografiat, de filmat; supravegherea domiciliului prin utilizarea mijloacelor tehnice; interceptarea convorbirilor telefonice şi a altor convorbiri; controlul comunicărilor telegrafice şi a altor comunicări; culegerea informaţiei de la instituţiile de telecomunicaţii); alte măsuri operative de investigaţii (chestionarea; culegerea informaţiei; urmărirea vizuală; urmărirea şi documentarea cu ajutorul metodelor şi mijloacelor tehnice moderne; colectarea mostrelor pentru cercetarea comparativă; efectuarea achiziţiilor de control şi a controlului livrărilor de mărfuri şi producţie aflate în circulaţie liberă sau limitată; cercetarea obiectelor şi actelor; identificarea persoanei; cercetarea încăperilor, clădirilor, porţiunilor de teren şi a mijloacelor de transport; cercetarea corespondenţei condamnaţilor; ţinerea convorbirilor; aplicarea detectorului comportamentului simulat; marcarea cu substanţe chimice şi alte substanţe speciale; experimentul operativ; infiltrarea operativă în organizaţiile criminale a colaboratorilor titulari din subdiviziunile operative şi a persoanelor care colaborează în mod confidenţial cu organele care exercită activitate operativă de investigaţii, utilizând acte de identitate şi alte documente de acoperire; controlul

[4] I. Covalciuc, „Reflexii asupra evoluției istorice a reglementărilor normative privind activitățile speciale de investigații”, în *Revista Națională de Drept*, nr. 11/2016, p. 57.

transmiterii banilor sau altor valori materiale extorcate; monitorizarea tranzacţiilor efectuate prin unul sau mai multe conturi bancare).

Problematica definirii regimului extrajudiciar al activităţii speciale de investigaţii a fost abordată[5], ca necesitate teoretico-practică de clarificare a următoarelor proceduri de bază: documentarea ca varietate de cunoaştere a fenomenelor lumii înconjurătoare; stabilirea adevărului obiectiv în calitate de scop al documentării; sarcinile şi obiectul documentării; sursele şi mijloacele documentării; conţinutul procesului de documentare; reglementarea juridică a documentării; particularităţile documentării în timpul realizării măsurilor operative de investigaţii. Despre documentare, ca mijloc de realizare a activităţilor speciale de investigaţii se apreciază că are rolul studierii şi descoperii modalităţilor de cunoaştere a adevărului realizabil, atât generic (declaraţii persoane vătămate, martori, concluzii specialişti, documente obţinute, urme fixate, înscrieri foto, audio, video sau alţi purtători de informaţii). De asemenea, are şi rolul specific prin norme certe şi regulamente departamentale, susţinute de teorie atât cunoaşterea materializată prin colectarea, verificarea, aprecierea şi fixarea, cât şi activitatea, prin folosirea rezultatelor obţinute în procedura judiciară, toate având caracter sistemic şi de concentrare a datelor operative despre persoană, fapte, trecut infracţional, legături, ca obiectiv esenţial în realizarea sarcinilor concrete activităţii speciale de investigaţii. Rezultă că dualitatea măsurilor speciale de investigare extrajudiciare şi convergenţa cu normele procesual penale sau de securitate naţională, este apreciată şi din perspectiva obiectelor ţintă şi anume: obiecte ce au legătură cu faptul infracţiunii, circumstanţele ce necesită a fi stabilite în cadrul unui dosar penal – obiect al probaţiunii, precum şi – colectarea de informaţii despre evenimente sau acţiuni care pun în pericol securitatea de stat normă reglementată diferit.

Este relevantă comparaţia: documentare prin activitate operativă de investigaţii – probatoriu prin măsuri procesual penale, susţinută din perspectiva asistării, prin cunoaşterea evenimentelor care au avut loc în trecut, a celor care se află în proces de pregătire sau în prezent se desfăşoară, precum şi a celor care datorită situaţiei create pot să survină în viitor. Este necesar a fi colectate şi informaţii de la participanţii la procedură (persoane care acordă asistenţă organelor operative de investigaţii sau colaboratorii operativi) privind actele pregătitoare sau în desfăşurare având posibilitatea urmăririi mijlocit sau nemijlocit a parcursului. Mărturia acestora ar duce la clarificarea fără dubiu a infracţiunii, fiind îndeplinit obiectivul probatoriului procesul penal determinat de circumstanţele ce urmează a fi dovedite în procesul penal şi anume: faptele referitoare la existenţa elementelor infracţiunii, precum şi cauzele care înlătură caracterul penal al faptei; circumstanţele prevăzute de lege care atenuează sau agravează răspunderea penală a făptuitorului; datele personale care caracterizează inculpatul şi victima; caracterul şi mărimea daunei cauzate prin infracţiune; existenţa bunurilor destinate sau

[5] I. Carlașuc, „Regimul extrajudiciar al activității operative de investigații în realizarea sarcinilor stabilite prin lege", în *Revista Teorii și practici de guvernări democratice*/ Materialele sesiunii de comunicări științifice 23-24.10.2010, Chișinău, [Online] la http: //iso.fd.md/caiet_site/caiet_nr. 4.pdf/pg.418-423, accesat 31.03.2019.

utilizate pentru săvârşirea infracţiunii sau dobândite prin infracţiune, indiferent cui au fost transmise; toate circumstanţele relevante la stabilirea pedepsei.

Garanţia respectării drepturilor şi libertăţilor fundamentale este susţinută prin concentrarea materialelor în dosarele de evidenţă operativă, utilizate în situaţiile de solicitare în vederea punerii în aplicare, extrajudiciar, a măsurilor operative care limitează drepturile constituţionale ale persoanelor, întemeiate pe date veridice, supuse autorizării judecătorului de instrucţie. Controlul judiciar al măsurilor speciale de investigaţii, prin faptul că verificările operative care vizează drepturile constituţionale ale persoanelor precum şi libertăţile fundamentale, se efectuează numai după autorizarea prealabilă a acestuia.

Fundamentarea statutului unic al judecătorului de instrucţie, conform normelor de procedură penală, în opinia autorului, îi conferă acestuia atribuţii proprii de urmărire penală, dar şi de control judiciar asupra acţiunilor procesuale efectuate în cadrul urmăririi penale.

Adoptarea Noilor Coduri Penale şi de Procedură Penală[6] au determinat reaşezarea activităţii speciale de investigaţii pe o altă lege, astfel, prin Legea nr. 59 din 29.03.2012[7], noţiunea este definită ca *„o procedură cu caracter secret şi/sau public, efectuată de autorităţile competente, cu sau fără utilizarea echipamentelor tehnice speciale, în scopul culegerii de informaţii, necesare pentru prevenirea şi combaterea criminalităţii, asigurarea securităţii statului, ordinii publice, apărarea drepturilor şi intereselor legitime ale persoanelor, descoperirea şi cercetarea infracţiunilor*". Activităţile sunt organizate în trei categorii distincte: *cu autorizarea judecătorului de instrucţie*: cercetarea domiciliului şi/sau instalarea în el a aparatelor ce asigură supravegherea şi înregistrarea audio şi video, a celor de fotografiat şi filmat; supravegherea domiciliului prin utilizarea mijloacelor tehnice ce asigură înregistrarea; interceptarea şi înregistrarea comunicărilor şi imaginilor; reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale; monitorizarea conexiunilor comunicaţiilor telegrafice şi electronice; monitorizarea sau controlul tranzacţiilor financiare şi accesul la informaţia financiară; documentarea cu ajutorul metodelor şi mijloacelor tehnice, precum şi localizarea sau urmărirea prin sistem de poziţionare globală ori prin alte mijloace tehnice; colectarea informaţiei de la furnizorii de servicii de comunicaţii electronice, toate aceste măsuri fiind autorizate a se efectua, la solicitarea procurorului, doar în cadrul unui dosar penal; *cu autorizarea procurorului*: identificarea abonatului, proprietarului sau a utilizatorului unui sistem de comunicaţii electronice ori al unui punct de acces la un sistem informatic; urmărirea vizuală; controlul transmiterii banilor sau altor valori materiale extorcate (doar în cadrul unui dosar penal); investigaţia sub acoperire; supravegherea transfrontalieră (doar în cadrul unui dosar penal); livrarea controlată (doar în cadrul unui dosar penal); colectarea mostrelor pentru cercetare comparată; cercetarea obiectelor şi a documentelor; achiziţia de control, cu excepţia

[6] Codul de procedură penală al Republicii Moldova (Cod nr. 122 din 14.03.2003), publicat în Monitorul Oficial al Republicii Moldova nr. 104-110 din 07.06.2003.

[7] Legea nr. 59 din 29.03.2012 privind activitatea specială de investigaţii, publicată în Monitorul Oficial al Republicii Moldova, nr. 113-118 din 08.06.2012.

a trei din acestea, toate celelalte fiind în formă dual judiciară şi extrajudiciară; *cu autorizarea conducătorului subdiviziunii specializate*: chestionarea; culegerea de date despre persoane şi fapte; identificarea persoanei, toate fiind efectuate ca şi activitate extrajudiciară.

Materia normativă extra-procesuală ce vizează activitatea specială de investigaţii a fost analizată în literatura de specialitate[8], în privinţa principiilor şi conţinutului acesteia. Principiile sunt *„ideile, tezele fundamentale care stau la baza întregului sistem de drept*" şi care se manifestă în (i) principii ce reflectă esenţa activităţii speciale de investigaţii şi trăsăturile specifice acesteia; (ii) principii care prin sine reprezintă un sistem de norme juridice, unice pentru întreaga activitate specială de investigaţii; dar şi pentru a determina ilegalitatea măsurilor speciale de investigaţii prin încălcarea principiilor acestei activităţi. Din punct de vedere teoretic, au fost trasate criterii în funcţie de gradul de concretizare şi gradul de răspândire. De apreciat ca esenţiale în ceea ce priveşte finalitatea activităţii speciale de investigaţii sunt: *principiile constituționale* ale activităţii speciale de investigaţii şi *alte principii ale activității* ce rezultă din legea cu privire la activitatea specială de investigaţii sau alte acte normative. Sub aspect gnoseologic, îndeplinirea dual a atribuţiilor ca finalitate în activitatea specială de investigaţii, se face astfel: a) *în cadrul procesului penal*: protejarea persoanei, societăţii şi statului de infracţiuni, precum şi protejarea persoanei şi societăţii de faptele ilegale ale persoanelor cu funcţii de răspundere în activitatea lor legată de cercetarea infracţiunilor presupuse sau săvârşite, astfel că orice persoană care a săvârşit o infracţiune să fie trasă la răspundere penală potrivit vinovăţiei sale şi nicio persoană nevinovată să nu fie trasă la răspundere penală sau condamnată; b) *în cadrul activității speciale de investigaţii*: culegerea de informaţii necesare pentru prevenirea şi combaterea criminalităţii, asigurarea securităţii statului, ordinii publice, apărarea drepturilor şi intereselor legitime ale persoanelor, descoperirea şi cercetarea infracţiunilor[9].

În analiza teoretico-practică a criteriilor de clasificare a măsurilor speciale de investigaţii au fost realizate o serie de analize, în care se apreciază ca importantă o astfel de activitate în scopul determinării temeiurilor şi condiţiilor de înfăptuire, activitate care în genere se bazează pe experienţa şi viziunea fiecărui specialist în domeniu. Astfel apreciem relevantă clasificarea raportată convenţional după cum urmează: a) după modul de realizare public - secret; b) după subiectul autorizării judecător de instrucţie-procuror-conducător al subdiviziunii specializate; c) după gradul de lezare al drepturilor şi libertăţilor omului: nu aduc atingere acestora – care încalcă aceste drepturi; d) după intensitatea utilizării mijloacelor tehnice speciale: măsuri speciale tehnice - preponderent cu utilizarea mijloacelor tehnice - fără aplicarea echipamentelor tehnice; e) după regimul lor juridic în măsuri: care se înfăptuiesc cu autorizarea judecătorului de instrucţie doar în cadrul unui proces

[8] V. Rusu, I. Covalciuc, „Unele reflecții asupra sistemului și conținutului principiilor activității speciale de investigații", în *Revista Națională de Drept*, nr. 8/2015, pp. 51-54.

[9] I. Covalciuc, „Actualitatea și importanța activității speciale de investigații în contextul ultimelor modificări legislative" în *Buletinul Științific al Univ. de Stat Bogdan Petriceicu Hașdeu, Științe sociale* nr. 2(4)/2016, p. 179.

penal - care se înfăptuiesc cu autorizarea procurorului doar în cadrul unui proces penal - care se înfăptuiesc cu autorizarea procurorului în cadrul unui proces penal cât şi în afara acestuia şi care se înfăptuiesc cu autorizarea conducătorului subdiviziunii specializate în afara procesului penal. În concluzie, autorul susţine că esenţa reglementării măsurilor speciale de investigaţii o constituie limitarea drepturilor omului, care determină şi categoria subiectului împuternicit cu dreptul de a o autoriza[10].

Sub aspect general, se afirmă despre activitatea specială de investigaţii, ca şi alte activităţi desfăşurate de organele statului, că este îndreptată spre ocrotirea ordinii de drept, fiind strict reglementată de lege şi că se realizează printr-un sistem de măsuri publice cât şi confidenţiale, având propriile trăsături specifice. Aceste trăsături sunt :

a) caracter de sine stătător – se manifestă prin faptul că în esenţă activitatea de investigaţii presupune utilizarea unor forţe, mijloace şi metode speciale, care după formă, conţinut şi origine diferă de cele specifice activităţii de urmărire penală, administrative; caracterul autonom este determinat şi de mecanismul reglementării normative al acestei activităţi;

b) stricta legiferare - prin lege organică sunt stabilite scopurile, sarcinile, principiile, măsurile speciale de investigaţii, temeiurile şi condiţiile înfăptuirii lor, sunt prevăzute organele abilitate cu drepturi şi obligaţii. Reglementarea strictă şi detaliată permite utilizarea complexă a forţelor şi mijloacelor din dotarea organelor speciale de investigaţie, aplicarea unor metode speciale de prevenire şi combatere a infracţiunilor, căutarea persoanelor care se ascund de organele de urmărire penală sau de instanţa de judecată ori care se eschivează de la executarea pedepsei penale, a persoanelor dispărute fără urmă, precum şi soluţionarea altor sarcini prevăzute de lege aspect ce serveşte ca garant pentru respectarea legalităţii în procesul exercitării activităţii speciale de investigaţii şi prevenirea încălcărilor drepturilor şi libertăţilor constituţionale ale cetăţenilor; c) realizarea de către organe special împuternicite - activitatea specială de investigaţii este exercitată de către subdiviziunile specializate ale Ministerului Afacerilor Interne, Ministerului Apărării, Centrului Naţional Anticorupţie, Serviciului de Informaţii şi Securitate, Serviciului de Protecţie şi Pază de Stat, Serviciului Vamal şi Departamentul Instituţiilor Penitenciare al Ministerului Justiţiei;

d) exercitarea numai în vederea atingerii scopurilor şi realizării sarcinilor prevăzute în lege - înfăptuirea măsurilor speciale de investigaţii pentru realizarea scopurilor şi sarcinilor neprevăzute de legea cu privire la activitatea specială de investigaţii, nu se admite.

Din perspectiva izvoarelor şi reglementărilor diferite, măsurile speciale de investigaţii judiciare şi extrajudiciare, a fost apreciat că, deşi ambele forme converg către un scop similar, garanţiile oferite le diferenţiază iar finalitatea acestora este

[10] I. Botnarii, „Nomenclatorul, criteriile de clasificare și categoriile măsurilor speciale de investigații", în *Revista Legea și Viața*, Martie 2018, p. 4042, și V. Mârzac, B. Glăvan, „Utilizarea mijloacelor tehnice în activitatea specială de investigații", Academia de Poliție Ștefan cel Mare, 2014.

cu totul alta. Prin măsurile extrajudiciare sunt colectate informaţii referitoare la intenţii criminale, pregătiri a unor acţiuni ilicite, ca formă incipientă sau de pregătire a unei infracţiuni, spre deosebire de cele judiciare care colectează elemente ce ţin de descoperirea infracţiunilor ca fapt material şi realizarea actului de justiţie[11].

În doctrina, se identifică posibilitatea persoanei vătămate într-un drept al său de către o autoritate publică, de a fi îndreptăţită să obţină recunoaşterea dreptului abuzat[12]. În cadrul unei astfel de realizări eficiente, se apreciază că se deschid la un nivel mai înalt pârghiile legale disponibile ţinându-se cont de actul de reglementare, astfel: a) norma procesuală: Codul de procedură penală care prevede o serie de drepturi şi libertăţi ce pot fi aparate prin contestarea acţiunilor şi actelor organelor de urmărire penală; b) norma constituţională: Constituţia care prevede drepturile şi libertăţile omului recunoscute ca fundamentale; c) norma internaţională: Convenţia Europeană pentru drepturile omului şi libertăţilor fundamentale şi alte acte internaţionale incidente, la care Republica Moldova este parte, normele internaţionale având prioritate în faţa normelor interne.

Importanţa judecătorului de instrucţie, ca subiect special împuternicit să exercite controlul judecătoresc în procedura prejudiciară este abstractizată ca sancţiune prin controlul prealabil al legalităţii şi temeiniciei actelor şi acţiunilor pe care trebuie să le înfăptuiască organul de urmărire penală, dar şi ca autorizare pentru acţiunile de urmărire penală care limitează inviolabilitatea persoanei, domiciliului, corespondenţei, convorbirilor telefonice, comunicărilor telefonice şi a altor comunicări şi alte acţiuni prevăzute de lege, prevăzute atât de normele procesual-penale cât şi de cele operativ-investigative, atât anterior şi ulterior materializării.

În privinţa diferenţierii ca procedură de examinare a materialelor ce confirmă necesitatea solicitării unor activităţi de îngrădire a drepturilor unei persoane sau de intruziune în proprietatea acesteia, se constată că măsurile speciale de investigaţii sunt aşezate pe recomandări de parcurs, iar normele procesuale au reglementări clare şi detaliate, susţinând ideea că măsurile operative de investigaţii ce limitează drepturi ocrotite prin lege să fie admise doar în scopul culegerii informaţiilor despre persoanele care pregătesc sau care atentează să comită infracţiuni grave.

Controlul asupra măsurilor speciale de investigaţii este văzut ca o condiţie obligatorie în scopul realizării obiectivelor specifice, sarcina de bază fiind legalitatea şi motivarea activităţilor investigativ-operative, cu respectarea drepturilor

[11] T. Osoianu, V. Orîndaş, *Procedură penală. Partea generală. Curs universitar*, Chişinău, 2004, p. 45.

[12] I. Dolea *et. al.*, *Tratat de drept procesual penal*, Editura Cartier Juridic, Chişinău, 2005, p. 605.

constituţionale ale persoanelor ce sunt sau urmează a fi îngrădite, atât în materie procesual-penală cât şi extra-procesuală[13].

Problematica măsurilor speciale de investigaţii a fost abordată şi în alte materiale de către autorul Dolea I.[14], fiind de părerea că aplicarea legislaţiei cu privire la activitatea operativă de investigaţii în cadrul procesului penal produce sincope, argumentând aspectul legat de valoarea probatorie a rezultatelor acestora prin asimilarea în categoria mijloacelor de probă şi respectarea condiţiilor de autenticitate şi posibilităţii de verificare aşa cum sunt enumerate în procedura penală.

În Tratatul *Comentariu aplicativ al Codului de procedură penală,* realizat de acelaşi autor, măsurile speciale de investigaţii sunt analizate în lumina modificărilor legislative, atât din perspectiva valorii probante cât şi din cea a garanţiilor asigurate de normele procesual penale. Autorul lasă să se înţeleagă că necesitatea intruziunilor în viaţa privată a unei persoane poate fi justificată numai dacă, printr-o altă măsură, mai puţin intruzivă, nu se poate aduce la îndeplinire scopul investigaţiei, fiind atins nivelul de exigenţă prevăzut de materia Curţii Europene.

Analizând conceptul juridic al măsurilor şi metodelor speciale de investigaţii, prin compararea normelor de reglementare, autorii Roman D. şi Popa S. apreciază că prin desfăşurarea activităţilor speciale de investigaţii prevăzute de Legea nr. 59/2012, în condiţiile Codului de procedura penală modificat prin Legea nr. 66/2012, acestea sunt asimilate şi definitoriu ca, *„totalitate de acţiuni de urmărire penală cu caracter public şi/sau secret efectuate de către ofiţerii de investigaţii în cadrul urmăririi penale numai în condiţiile şi în modul prevăzut de cod, aşa cum sunt prevăzute în dispoziţiile generale privind activitatea specială de investigaţii*" (Art. 132[1] alin. (1) din C.pr.pen. al R.M.).

În această situaţie, s-a identificat un conflict al definiţiilor prin faptul că norma procesual-penală priveşte acţiuni de urmărire penală efectuate doar după începerea urmăririi penale. Norma specială priveşte posibilitatea efectuării măsurilor speciale de investigaţii atât în cadrul procesului penal cât şi în afara acestuia autorii prezumând că anumite măsuri speciale de investigaţii urmează a fi efectuate după înregistrarea infracţiunii, până la începerea urmăririi penale, în termenul legal, iar anumite măsuri speciale de investigaţii pot fi efectuate numai după începerea urmăririi penale, conform prevederilor C.pr.pen. R.M., fiind create impedimente în aplicarea eficientă a legii în activitatea de prevenire, depistare şi investigare a infracţiunilor. În acest sens, au definit *„activitatea specială de investigaţii, ca totalitatea de procedee probatorii cu caracter secret şi/sau public, efectuate de autorităţile competente, până la sesizarea/autosesizarea organelor de drept, în cadrul procesului penal şi/sau urmăririi penale, în scopul culegerii de informaţii necesare*

[13] V. Moraru, I. Covalciuc, „Particularitățile exercitării controlului asupra măsurilor speciale de investigații autorizate de către procuror", în *Revista Legea și Viața*, nr. 12/2016, p. 47.

[14] I. Dolea, *Drepturile persoanei în probatoriul penal. Concepția promovării elementului privat*, Editura Cartea Juridică, Chișinău, 2009, p. 168.

pentru prevenirea şi combaterea criminalităţii, asigurarea securităţii statului, ordinii publice, apărarea drepturilor şi intereselor legitime ale persoanelor, descoperirea şi cercetarea infracţiunilor".

Pentru a evidenţia şi din perspectivă teoretică măsurile speciale de investigaţii definite generic în procedura penală, au reliefat că acestea au ca element concret, metoda, care le determină conţinutul şi care prin elementul tactic clasificat, le diferenţiază de urmărirea penală. Exemplificând pe forma legii, autorii au asociat măsuri speciale şi metode tactice, astfel, măsura specială, urmărirea vizuală, are ca metodă urmărirea, supravegherea operativă nemijlocită, iar metoda, informare electronică, poate fi aplicată limitat şi condiţionat de obiectul ţintă şi mijloacele tehnice folosite[15].

Este de interes modalitatea în care autorii au abordat una din sarcinile activităţii speciale de investigaţii, şi anume relevarea atentatelor criminale, prevenirea, curmarea infracţiunilor şi identificarea persoanelor care le organizează şi/sau comit. Astfel, indiferent pe care direcţie s-ar merge, în sensul conţinutului sarcinii, identificarea persoanei este esenţială, iar pentru îndeplinirea sarcinii este necesar a se efectua un cumul de activităţi speciale informativ-operative precum şi de căutare-identificare. A fost evidenţiată diferenţa dintre *identificarea persoanei prin măsuri speciale de investigaţii*, ca identificare neprocesuală şi *procedura activităţii prezentării pentru recunoaştere*, şi care permite în scopul realizării, utilizarea diferitelor metode şi mijloace de stabilire a identităţii, ambele având în comun metodele identificării criminalistice. A fost realizată o clasificare a elementelor, ca acţiuni în scopul identificării persoanelor şi a felurilor identificării, astfel, primele fiind materializate prin acţiuni de acumulare a informaţiei, cu obiect bine determinat şi acţiuni ce stabilesc asemănarea cu obiectul de identificat, care pot fi elemente ale măsurii de identificare a persoanei sau elemente pentru alte măsuri speciale, iar secundele, prin nemijlocite/mediate, public/cifrat sau secret.

Relevantă este concluzia autorilor materialului, în sensul că, pentru organele de anchetă, identificarea persoanei prin măsuri şi metode speciale este oportună şi necesară în situaţia în care autorul unei infracţiuni nu poate fi altfel identificat, rezultatele obţinute având rolul de a oferi sprijin pentru căutarea probelor şi stabilirea căilor de investigaţie, exclus fiind recunoaşterea acestora ca probe în procesul penal[16].

Utilizarea măsurilor operative de investigaţii în activitatea de prevenire şi combatere a faptelor de corupţie, ca fenomen antisocial, ce posedă o individualitate bine marcată, atât juridico-penal cât şi a particularităţilor tacticii şi metodologiei descoperirii, fiind strâns legată inclusiv de crima organizată, ce pune în pericol valorile democratice, inclusiv drepturile şi libertăţile fundamentale ale omului şi buna funcţionare a instituţiilor statului. Cu privire la activitatea de investigare-cercetare a evidenţiat diversitatea modalităţilor de efectuare a unei urmăriri penale

[15] D. Roman, S. Popa, „Identificarea persoanei prin măsuri și metode speciale de investigații", în *Studia Universitatis Moldaviae*, Seria științe juridice, nr. 3 (103)/2018, pp. 193-195.

[16] *Idem*, pp. 196- 200.

complexe prin îmbinarea măsurilor operative de investigaţii cu alte procedee extrajudiciare, în scopul unic de aflare a adevărului. În opinia sa, criminalistica este vitală, deoarece, prin utilizarea tuturor mijloacelor tehnico-ştiinţifice, tactice şi metodologice, bazate pe o planificare judicioasă în care se prevede cu exactitate locul efectuării actelor de investigare, momentele specifice cazului concret şi caracteristicile persoanelor implicate la realizarea lor, se acumulează materialul probator atât pentru faptele reconstituite cât şi flagrante. Despre testarea poligraf, ca o măsură operativă de investigaţii, remarcă faptul că rezultatul nu constituie mijloc de probă, dar în genere este utilizat la pregătirea unei anchete penale, ca date de interes în efectuarea a unor măsuri operative de investigaţii, iar ca probă doar cu respectarea prevederilor C.pr.pen. R.M., nerespectarea condiţiei imperative determinând încălcarea principiului prezumţiei de nevinovăţie[17].

Aşa cum remarcă autorii Cobîrşenco I. şi Fala M.[18], proporţionalitatea semnifică *un echilibru just şi imperativ de menţinut între intruziunea în viaţa privată a persoanei şi importanţa faptică privind o anchetă, astfel încât autorizarea unei măsuri să se facă în concordanţă cu gravitatea faptei.*

În materia respectării *secretului corespondenţei*, sunt evocate garanţiile constituţionale privind secretul scrisorilor, telegramelor, altor trimiteri poştale, al convorbirilor telefonice şi al celorlalte mijloace legale de comunicare dar şi norma de excepţie, derogare naţională, ingerinţa necesară în interesele securităţii naţionale, bunăstării economice a ţării, ordinii publice şi în scopul prevenirii infracţiunilor. În materia garanţiilor internaţionale, articolul 8 alin. (2) CEDO, menţionează că *„nu este admis amestecul unei autorităţi publice în exercitarea acestui drept decât în măsura în care acest amestec este prevăzut de lege şi dacă constituie o măsură care, într-o societate democratică, este necesară pentru securitatea naţională, siguranţa publică, bunăstarea economică a ţării, apărarea ordinii şi prevenirea faptelor penale, protejarea sănătăţii sau a moralei, ori protejarea drepturilor şi libertăţilor altora*", prevedere care este generatoare atât de drept cât şi de obligaţie. Ca prim procedeu de probaţiune, în Codul de procedură penală se menţionează că dreptul la secretul scrisorilor, al telegramelor, altor trimiteri poştale, convorbirilor telefonice şi al celorlalte mijloace legale de comunicare este asigurat de stat. Limitarea acestui drept se admite numai în baza unui mandat judiciar emis în condiţiile legii. Ţinând cont de faptul că procesul penal are ca scop protejarea persoanei, societăţii şi statului de infracţiuni, precum şi protejarea persoanei şi societăţii de faptele ilegale ale persoanelor cu funcţii de răspundere în activitatea lor legată de cercetarea infracţiunilor presupuse sau săvârşite, este necesar ca organul de urmărire penală în procesul urmăririi penale să efectueze un anumit număr de acţiuni procesuale, ca necesare cu privire la stabilirea existenţei infracţiunii, identificarea făptuitorului şi a se constata dacă este sau nu cazul să se transmită cauza penală în judecată în condiţiile legii.

[17] V. Cuşnir, *Corupția. Reglementare de drept, activități de prevenire și combatere. Partea I*, Academia de Poliție Ștefan cel Mare, Chișinău, 1999, pp. 83-138.

[18] I. Cobîrșenco, M. Fală, „Principiul proporționalității măsurilor special de investigații. Garanția dreptului la viață privată", în *Revista Națională de Drept*, nr. 12/2017, p. 4856.

Un procedeu probatoriu secund prin care organul de urmărire penală poate administra probe este cel privind măsurile speciale de investigaţii întreprinse în cadrul activităţii speciale de investigaţii. În înţelesul Recomandării (2005) 10 a Comitetului de Miniştri al Consiliului Europei, prin noţiunea de tehnici speciale de investigare se înţelege *tehnicile aplicate de autorităţile competente în cadrul anchetelor penale, vizând depistarea sau anchetarea unor infracţiuni grave şi a unor suspecţi în vederea colectării de informaţii, de aşa manieră încât persoanele în cauză să nu aibă cunoştinţă de acest lucru.* Întrucât asemenea definire se regăseşte şi în art. 132 alin. (1) C.pr.pen. R.M., autorii apreciază că situaţia în cauză este în prezenţa a două legi, ambele conţinând norme cu privire la activitatea specială de investigaţii, însă, în conformitate cu art. 2 alin. (4) C.pr.pen., normele juridice cu caracter procesual din alte legi naţionale pot fi aplicate numai cu condiţia includerii lor în C.pr.pen.

Sunt enumerate măsurile speciale de investigaţii care aduc atingere nemijlocit dreptului secretului corespondenţei: interceptarea şi înregistrarea comunicărilor sau a imaginilor; reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale; monitorizarea conexiunilor comunicaţiilor telegrafice şi electronice; monitorizarea sau controlul tranzacţiilor financiare şi accesul la informaţia financiară; colectarea informaţiei de la furnizorii de servicii de comunicaţii electronice. Pentru ca aceste măsuri să aibă un caracter legal, este necesar să fie îndeplinite următoarele condiţii: a) este imposibilă realizarea scopului procesului penal şi/sau poate fi prejudiciată considerabil activitatea de administrare a probelor; b) există o bănuială rezonabilă cu privire la pregătirea sau săvârşirea unei infracţiuni grave, deosebit de gravă sau excepţional de gravă, cu excepţiile stabilite de lege; c) acţiunea este necesară şi proporţională cu restrângerea drepturilor şi libertăţilor fundamentale ale omului.

Cu referire la aceleaşi criterii de stabilire a proporţionalităţii, autorii abordează şi *dreptul la inviolabilitatea domiciliului*, în cadrul efectuării măsurilor speciale de investigaţii, astfel de la norma constituţională se poate deroga prin lege, pentru: executarea unor mandate de arestare sau a unei hotărâri judecătoreşti; înlăturarea unei primejdii care ameninţă viaţă, integritatea fizică sau bunurile unei persoane; prevenirea răspândirii unei epidemii. Materia procesual penală permite efectuarea percheziţiilor, cercetării domiciliului, care sunt ordonate şi efectuate în baza unor mandate judiciare iar cu privire la măsurile speciale de investigaţii ce aduc atingere acestui drept, organele de urmărire penală sunt în drept a efectua: cercetarea domiciliului şi/sau instalarea în el a aparatelor ce asigură supravegherea şi înregistrarea audio şi video, a celor de fotografiat şi de filmat; supravegherea domiciliului prin utilizarea mijloacelor tehnice ce asigură înregistrarea; investigaţia sub acoperire, care în mod obligatoriu se materializează în documente şi sunt supuse anumitor termene. Se concluzionează că principiul proporţionalităţii între dreptul sau libertatea persoanei garantate de lege şi necesitatea efectuării acţiunii procesuale solicitate recunoaşte că drepturile omului nu sunt absolute şi exercitarea drepturilor unei persoane trebuie să fie apreciată în raport cu interesul

public mai larg, statele bucurându-se de o anumită marjă de apreciere în materia impunerii unor restricţii, marjă care nu este nelimitată.

Este interesantă abordarea autorului Copeţchi S.[19], care în mod obiectiv analizează situaţia investigatorului sub acoperire, ca ofiţer de investigaţii antrenat în realizarea investigaţiei, fiind în acord cu prevederile art. 30 alin. (4) din Legea M.S.I., unde sunt definiţi ca angajaţi special desemnaţi din cadrul M.A.I., S.I.S., C.A.N., Departamentul Instituţiilor penitenciare din cadrul Ministerului Justiţiei. Ofiţerul de investigaţii, în exercitarea atribuţiilor de culegere a datelor şi informaţiilor despre pregătirea ori comiterea unei infracţiuni, poate determina prin comportamentul său acţiuni, situaţie care generează depăşirea limitelor de competenţă, rolul acestuia fiind de a observa discret. S-a potenţat diferenţa între provocare şi folosirea tehnicilor legale în activităţile specifice sub acoperite în cadrul dosarelor penale, clarificări în acest sens materializându-se oficial prin Hotărârea Plenului CSJ a R.M. nr. 11/22.12.2014 cu privire la aplicarea legislaţiei referitoare la răspunderea penală pentru infracţiunile de corupţie, în materia condiţiilor în care trebuie reţinută provocarea. Aceste condiţii sunt: acţiunea presupusă ca act de corupere să fie probată prin solicitarea venită de la persoana care avea atribuţia descoperirii infracţiunii sau există o determinare directă de la un denunţător; fapta nu s-ar fi comis fără intervenţia provocării; nu există suspiciuni anterioare privind implicarea în fapte de corupţie. Curtea apreciază că *statul trebuie să descopere infracțiuni, nu să încurajeze săvârşirea acestora, astfel în mod inadmisibil există riscul provocării unei persoane nevinovate, recunoscând-o fictiv ca vinovată de faptă.*

În aceeaşi ordine de idei, analizând raţionamentele art. 6, part. 1 CEDO referitoare la acţiunile de provocare organizată, Eni A[20]. apreciază că acestea pot îmbrăca forma instigării la săvârşirea de infracţiuni, abordându-se în acest sens garanţii suplimentare dreptului persoanei de a nu fi judecată în baza probelor acumulate. S-a argumentat exemplificând cu hotărâri CtEDO ce vizează cetăţeni ai R.M.: (i) în cauza Sandu contra Republicii Moldova unde o persoană a acţionat sub conducerea poliţiei ca o persoană privată (fără a avea investirea legală), iar acţiunile acesteia aveau trăsăturile unei investigaţii sub acoperire, caracterul provocator al comportamentului său fiind cercetat ca şi o provocare la săvârşirea infracţiunii din partea unui agent public – investigator sub acoperire; (ii) cauza Morari contra Republicii Moldova, care este realizată de către agenţii publici sub acoperire, adică angajaţi, special desemnaţi în acest scop, din cadrul Ministerului Afacerilor Interne.

Manualul judecătorului pentru cauze penale[21] are ca punct de plecare necesitatea ca orice proces să aibă la bază principiul respectării demnităţii umane

[19] S. Copeţchi, „Provocarea infracțiunii în contextul măsurilor speciale de investigații”, în *Revista Institutului Național al Justiției*, nr. 2(41)/2017, p. 2732.

[20] A. Eni, „Analiza hotărârilor CtEDO adoptate în privința Republicii Moldova în materia admisibilității tehnicilor de utilizate în operațiunile sub acoperire în cadrul investigațiilor penale”, în *Revista Studia Universitas Moldaviae*, nr. 8 (118)/2018, p. 8091.

[21] M. Poalelungi, I. Dolea *et. al.*, *Manualul judecătorului pentru cauze penale*, Chișinău, 2013, p. 1192.

(statul devenind responsabil pentru orice act care îi lezează drepturile şi libertăţile fundamentale cetăţeanului; prezumţia de nevinovăţie însoţind orice demers, judecătorul adoptând un anumit tip de comportament). Se instituie astfel un veritabil sistem de garanţii procesuale în materie penală, de fiecare dată acţiunile sale bazându-se pe reguli cu caracter general în aprecierea unor situaţii cu caracter specific.

În România, tehnicile speciale de supraveghere sau cercetare constituie o categorie de procedee probatorii şi măsuri de investigaţie cu caracter derogatoriu de la regulile de drept comun privind administrarea probelor, fiind recunoscute la nivel internaţional ca un instrument în combaterea infracţionalităţii de mare gravitate. Chiar dacă o parte din aceste tehnici erau cunoscute şi întrebuinţate în procesul penal de mai mult timp, chiar fiind prevăzute în recomandări şi convenţii internaţionale, legiuitorul român a preluat noţiunea de *tehnici speciale de investigare* în urma Recomandării (2005) 10 a Comitetului de Miniştri al Consiliului Europei[22].

Din definiţia dată de către Comitet se reţine că: *„prin tehnici special de investigare, se înţeleg tehnicile aplicate de autorităţile competente în contextual investigaţiilor penale în scopul descoperirii şi cercetării infracţiunilor grave şi a suspecţilor, în vederea colectării informaţiilor astfel de o manieră în care să nu alerteze persoanele vizate de aceste tehnici*". Din această definiţie rezultă două aspecte importante şi anume: necesitatea restrângerii folosirii tehnicilor speciale de investigare numai la infracţiunile grave şi caracterul secret al acestora[23].

Măsurile de supraveghere tehnică reprezintă una dintre cele mai severe intruziuni în viaţa privată a persoanei, astfel că s-a urmărit corelarea legislaţiei procesual-penale la aceste metode investigative moderne, demersuri destinate asigurării conformităţii între reglementarea procesual-penală şi exigenţele legii fundamentale, astfel cum acestea sunt edictate în Constituţia României precum şi cu cerinţele normative şi jurisprudenţiale izvorâte din articolul 8 al Convenţiei europene a drepturilor omului. În acest proces de elaborare a legislaţiei corespunzătoare, aflat într-o continuă dinamică determinată de evoluţia atât a metodelor tehnice, dar şi a viziunii Curţii Europene de Drepturilor Omului asupra metodelor de cercetare specială, principala dificultate a fost şi este reprezentată de găsirea unui cadru normativ adecvat, simplu şi predictibil, care să satisfacă necesitatea combaterii şi descoperirii infracţiunilor, dar şi să limiteze ingerinţa în drepturile fundamentale ale persoanei.

Apreciem că se impune a se menţiona faptul ca în mod frecvent se utilizează termenii de *măsură* şi *tehnică*, ambele făcând referire la acelaşi obiect, situaţie în care susţinem că nu se creează nicio diferenţiere, cu toate că la nivel internaţional este uzitat cu o mai mare frecvenţă termenul de *tehnică*.

[22] Recomandarea (2005) 10 a Comitetului de Ministri a Europei adoptata de Comitetul de Ministri la data de 20.04.2005.

[23] N. Bradley, "Evidence, special investigative techniques the right to a fair hearing", în *Revista ERA Forum*, vol.15, nr. 1/2014, p. 37.

În doctrină, s-a arătat faptul că tehnicile speciale de investigare sunt *procedee probatorii cu caracter derogatoriu, cu reguli şi proceduri particulare de autorizare, dar şi de punere în aplicare*[24]. Ţinând cont de sfera de aplicare şi natura fiecăreia, acestea au şi un caracter propriu, eterogen[25], aspect apreciat ca favorabil prin reglementarea clară şi delimitarea de procedeele comune întrucât acestea reprezintă o mare ingerinţa în viaţa privată a unei persoane[27]. S-a mai apreciat că spre deosebire de prevederile anterioare, legislaţia procesual-penală actuală realizează o buna sistematizare a acestora, uşurând aplicarea de către organele de urmărire penală, necesita o mai mare abstractizare şi o mai mare coerenta în reglementare.

În literatura de specialitate, s-a apreciat că pentru realizarea scopului procesului penal, acesta este călăuzit de reguli fundamentale ce fixează cadrul juridic care stabileşte limitele în care societatea trebuie să reacţioneze faţă de cei care încalcă legea penală[26].

Codul de procedura penală român[27] actual foloseşte noţiunile de *probă* şi *mijloc de probă*, la care se adaugă şi reglementarea unor *procedee probatorii* fără însă a le defini ca atare, aşa cum arată Titlul IV dar şi Capitolul IV Metode speciale de supraveghere sau cercetare.

În această situaţie şi metodele speciale de supraveghere sau cercetare se subordonează principiilor care guvernează procesul penal. Acestea sunt reglementate de prevederile articolele 212 din noul C.pr.pen Rom.[28], fiind următoarele: principiul legalităţii procesului penal, principiul separării funcţiilor judiciare, prezumţia de nevinovăţie, principiul aflării adevărului, principiul *ne bis în idem,* principiul oficialităţii procesului penal, caracterul echitabil şi termenul rezonabil al procesului penal, garantarea dreptului la libertate şi siguranţă, garantarea dreptului la apărare, respectarea demnităţii umane şi a vieţii private, desfăşurarea procesului penal în limba română şi dreptul la asistenţă gratuită din partea unui interpret. În afară de acestea, există principii sau trăsături specifice aplicabile numai în faza de urmărire penală, respectiv numai în faza de judecată.

Alţi autori[29] consideră că principiile specifice fazei de urmărire penală sunt în număr de trei, respectiv caracterul nepublic, caracterul necontradictoriu şi caracterul preponderent scris al urmăririi penale. La acestea alţi autori[30] adaugă şi un al patrulea principiu, respectiv subordonarea ierarhică în efectuarea actelor de

[24] G. Mateuț., *Procedura penală*, Editura Universul Juridic, București, 2019, p. 1075.

[25] M. Bulancea, G. Zlati, R. Slăvoiu, în M. Udroiu (coordonator), *Codul de procedură penală*, Editura C.H. Beck, Bucureşti, 2017, p. 2571.

[26] G. Mateuț, „Observații critice privind noua reglementare a supravegherii tehnice într-o perspectivă comparativă", în *Caiete de Drept Penal*, nr. 3/2015, p. 13.

[27] I. Neagu, *Drept procesual penal. Partea generală*, București, 1981.

[28] Legea nr. 135/2010 privind Codul penal și Codul de procedură penală al României, publicată în Monitorul oficial nr. 486 din 15.06.2010.

[29] M. Udroiu, *Procedură penală. Partea specială,* ed. 3, Editura C.H. Beck, București, 2016, p. 23.

[30] N. Volonciu, *Tratat de procedură penală, vol. 2,* Editura Paideia, București, 1996, p. 1112.

urmărire penală. Dintre acestea, doar caracterul nepublic al urmăririi penale a primit o consacrare legală expresă, prin prevederile articolul 285 alin. (2) C.pr.pen. Rom.

Principiul legalităţii este reglementat în cuprinsul articolul 2 din C.pr.pen Rom. şi prevede că procesul penal se desfăşoară potrivit dispoziţiilor prevăzute în lege, aspect ce presupune ca legea trebuie să fie conformă cu standardele constituţionale şi de protecţie a drepturilor omului, fiind necesar ca acţiunile desfăşurate de organele judiciare să fie conforme cu prevederile legale.

În doctrină[31], se mai face distincţia între legalitatea aplicabilă în majoritatea situaţiilor şi cea de excepţie care reprezintă o derogare prevăzută de lege de la principiul legalităţii, astfel ca actul efectuat în aceste condiţii nu înfrânge acest principiu.

Verificarea conformităţii cu normele constituţionale a generat o serie de interpretări. Astfel, s-a reţinut posibilitatea de a se putea verifica, din perspective nulităţii absolute, în faza judecăţii, dacă au fost respectate principiile legalităţii şi loialităţii administrării probelor, datorită regulii generale de a se invoca acest gen de nulitate în tot cursul procesului penal, iar în cazul unei astfel de constatări se va proceda la excluderea şi înlăturarea acestora din materialul probator al cauzei[32].

Principiu fundamental al loialităţii administrării probelor procesului penal are rolul de a opri folosirea de metode interzise cu scopul precis de a se obţine probe. Loialitatea probelor instituie de asemenea interdicţia şi în ceea ce priveşte folosirea provocării în scopul probării faptelor.

Autorul R.P. Răileanu[33] a apreciat că în mod excepţional probele administrate cu încălcarea prevederilor legale (excepţie tortura şi tratamentele inumane sau degradante) pot fi folosite în procesele penale dacă prin aceasta nu se aduce atingere caracterului echitabil al procedurii în ansamblu.

În jurisprudenţa CtEDO[34] s-a apreciat ca provocarea la comiterea unei infracţiuni are loc atunci când agenţii statului nu au un comportament pasiv, ci incita comiterea unei infracţiuni o persoana care altfel nu ar fi comise, fiind importante motivele care au stat la baza deciziei de iniţiere a măsurii special şi a comportamentului agenţilor statului.

În scopul de a se afla adevărul, organele judiciare au îndatorirea de a face demersuri în acest sens prin administrarea probelor care sunt necesare lămuririi pe deplin a tuturor aspectelor cauzei, inclusiv prin utilizarea măsurilor speciale de supraveghere sau cercetare, atunci când nu există o altă posibilitate. Tot în aceeaşi virtute, utilizând şi principiul libertăţii probelor se acordă posibilitatea părţilor de a solicita administrarea de probe pe care le apreciază ca fiind utile şi concludente în vederea soluţionării cauzei, situaţie în care se impune a mai adaugă şi faptul că,

[31] V. Dongoroz *et. al.*, *Explicații teoretice ale Codului de procedură penală român. Partea generală*, București, 1975.

[32] Decizia nr. 802/2017 publicată în Monitorul Oficial nr. 116 din 06.02.2018.

[33] R.P. Răileanu, „Principiile fundamentale ale procesului penal român în lumina noului cod de procedura penală", în Revista *Dreptul*, nr. 6/2014, p. 106.

[34] Cauza Pătraşcu contra României.

în general părţile deţin mai multe informaţii despre împrejurările de fapt care se urmăresc a fi stabilite.

În doctrină[35] s-a considerat că aflarea adevărului este unul dintre obiectivele administrării de probe, fiind rezultatul clarificării cauzei sub toate aspectele, pe baza de probe.

Prin Codul de procedură penală român în vigoare, legiuitorul a urmărit să unifice procedeele probatorii cu caracter derogatoriu şi intruziv sub o singura formă de reglementare cu caracter unitar[36], condiţiile rămânând egale dar procedurile de autorizare fiind diferite, unele fiind în competenta judecătorului de drepturi şi libertăţi iar altele la aprecierea procurorului.

Diferenţa între măsurile speciale de supraveghere şi măsurile speciale de cercetare nu este enunţată în cod, fiind lăsată la latitudinea doctrinei, urmare a menţiunii din cuprinsul articolul 138 alin. (13) C.pr.pen. Rom., în care se arată că prin supraveghere tehnică se înţelege utilizarea uneia dintre metodele prevăzute la alin. (1) li. a)-d.

Astfel, sunt considerate *metode speciale de supraveghere*: interceptarea comunicaţiilor ori a oricărui tip de comunicare la distanţă; accesul la un sistem informatic; supravegherea video, audio sau prin fotografiere; localizarea sau urmărirea prin mijloace tehnice, iar *metode speciale de cercetare* : obţinerea datelor privind tranzacţiile financiare ale unei persoane; reţinerea, predarea sau percheziţionarea trimiterilor poştale; utilizarea investigatorilor sub acoperire şi a colaboratorilor; participarea autorizată la anumite activităţi; livrarea supravegheată.

Diferenţa dintre metodele speciale de supraveghere şi metodele speciale de cercetare ar putea fi stabilită prin utilizarea criteriului referitor la faptul că, în cazul măsurilor de supraveghere, organele de urmărire penală primesc informaţiile chiar în timp ce se desfăşoară activităţile, dar în cazul măsurilor speciale de cercetare, organele de urmărire penală primesc informaţiile despre activităţi, după ce acestea au avut loc.

În vederea interpretării logice a limitelor între metodele speciale de supraveghere şi metodele speciale de cercetare, au fost identificate caracteristici care oferă clarificări şi utilitate stadiului actual de utilizare a tehnicilor speciale de investigare. Astfel a fost realizată o clasificare după 1) organul care autorizează măsura judecător de drepturi sau libertăţi sau procuror, 2) nivelul de intruziune în viaţa privată a unei persoane, 3) tipul de activitate, în timp real sau după consumarea faptelor, 4) complexitatea activităţii[37]. Or, tot în doctrină s-a susţinut necesitatea punerii în valoare a judecătorului, ca unic garant viabil al respectării drepturilor şi libertăţilor persoanei în cadrul unui proces penal[38].

---

[35] G. Antoniu, „Observaţii la proiectul noului Cod de procedura penală", în *Revista de drept penal*, nr. 1/2009.

[36] M. Udroiu, R. Slăvoiu, O. Predescu, *Tehnici speciale de investigare în justiţia penală*, Editura C.H. Beck, Bucureşti, 2009, p. 225.

[37] *Ibidem*, pp. 304-305.

[38] G. Mateuţ, Observaţii critice ..., *op. cit.*, p. 13.

Se poate concluziona cu faptul că se impune stabilirea de condiţii universale pentru toate tehnicile speciale de investigare, condiţiile referitoare la existenţa unei urmăriri penale începute (*in rem* sau *in personam*), respectarea proporţionalităţii măsurii cu scopul urmărit şi subsidiaritatea acesteia faţă de alte procedee probatorii mai puţin intruzive.

Interceptarea comunicaţiilor ori a oricărui tip de comunicare la distanţa a fost definită în doctrină[39] ca fiind *o măsură de supraveghere care include atât interceptarea propriu-zisă, cât şi activităţile conexe acces, monitorizare, colectare sau înregistrare, necesare pentru a transforma conţinutul unei comunicări într-un mijloc de probă.*

Accesul la un sistem informatic presupune căutarea şi identificare probelor aflate întruna dispozitiv de prelucrare automată a datelor calculator, tabletă, telefon, sau intru mijloc de stocare hard disk, cd, memory stick, prin folosirea de procedee tehnice care asigură confidenţialitatea acestui demers.

Supravegherea video, audio sau prin fotografiere reprezintă monitorizarea unei persoane şi înregistrarea imaginilor şi sunetelor surprinse cu această ocazie, asigurându-se în acest fel şi comunicările verbale sau mimico-gestuale.

Localizarea sau urmărirea prin mijloace tehnice este o activitate de monitorizare în timp real a deplasărilor pe care le efectuează o persoana, prin folosirea de dispozitive ataşate unor obiecte. Finalitatea acestei masuri este de a se stabili locul unde se afla sau unde efectuează deplasări o persoana.

Obţinerea de date privind tranzacţiile financiare este o măsură prin care se obţin date despre operaţiunile pe care o persoană le efectuează prin intermediul unei instituţii de credit, vizându-se atât tranzacţiile efective cat şi înscrisurile prin care se realizează.

În literatura de specialitate[40], s-a menţionat că prin aceasta măsură se pot obţine şi conţinutul tranzacţiilor efectuate, IP-urile folosite în logarea în anumite aplicaţii Internet Banking, precum şi date la care a fost folosit serviciul.

Percheziţia trimiterilor poştale reprezintă verificarea conţinutului scrisorilor sau al coletelor transmise prin poştă sau curierat, activitate desfăşurată fără ştiinţa expeditorului sau a destinatarului.

Obţinerea datelor generate sau prelucrate de către furnizorii de reţele publice de comunicaţii ori furnizorii de servicii de comunicaţii electronice destinate publicului, reprezintă un procedeu prin care organele de cercetare penală intră în posesia datelor de identificare ale comunicării, percepută ca orice schimb de informaţii realizat prin intermediul unei reţele publice de comunicaţii electronice.

Supravegherea tehnică reprezintă aplicarea oricăror procedee incluse în aceasta categorie: interceptarea comunicaţiilor ori ale comunicării, accesul la un sistem informatic, supravegherea video, audio sau prin fotografiere, localizarea sau urmărirea prin mijloace tehnice. Se dispune de către judecătorul de drepturi şi libertăţi la solicitarea organului judiciar, dacă sunt îndeplinite cumulativ

[39] M. Bulancea, G. Zlati, R. Slăvoiu, în M. Udroiu (coordonator), *op. cit.*, p. 2571.
[40] *Ibidem*, p. 653.

următoarele condiţii: exista o suspiciune rezonabila cu privire la pregătirea sau săvârşirea unei infracţiuni dintre cele prevăzute în mod explicit (alin. (2)); măsura este proporţională cu restrângerea drepturilor şi libertăţilor fundamentale date fiind particularităţile cauzei, importanţa informaţiilor ori a probelor ce urmează a fi obţinute sau gravitatea infracţiunii; probele nu ar putea fi obţinute în alt mod sau obţinerea lor ar presupune dificultăţi deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranţa persoanelor sau a unor bunuri de valoare.

Înregistrările la care face referire articolul 139 alin. (3) C.pr.pen. Rom. efectuate de părţi sau de alte persoane, constituie mijloc de probă când privesc propriile convorbiri sau comunicări pe care le-au purtat cu terţii. Orice alte înregistrări pot constitui mijloace de probă dacă nu sunt interzise prin lege.

Apreciem progresul legislativ, prin raportare la vechile norme procesual penale, prin aceea că a fost instituită procedura unitară de autorizare a măsurilor de supraveghere tehnică, în care rolul principal îl are judecătorul de drepturi şi libertăţi, de asemenea şi norma juridică este superioară prin aceea că nu transpune procedura interceptărilor şi înregistrărilor la alte măsuri de supraveghere tehnică, ci prevede că va trebui ca, pentru fiecare dintre măsuri să se procedeze la o analiză distinct, prin raportare la criteriile generale prevăzute la art. 139 C.pr.pen. Rom.

Concluzii

Reglementările legislative în vigoare în Republicii Moldova la capitolul măsurilor speciale de investigaţii îşi au sediul, atât în Codul de procedură penală, urmărind scopul soluţionării problemelor procesului penal, prin asigurarea probaţiunii urmăririi penale, cât şi în Legea specială nr. 59/2012 ca activităţi extra procesuale.

Reglementările legislative în vigoare în România la capitolul metodelor speciale de supraveghere sau cercetare sunt cuprinse exclusiv în Codul de procedură penală, în acest fel, legiuitorul urmărind realizarea probaţiunii în urmărirea penală şi implicit scopul procesului penal, prin asigurarea cadrului justificativ. Acestea sunt verificate periodic, urmare a sesizărilor transmise de diferite instanţe, sub aspectul încadrării în normele superioare protejate de către Curtea Constituţională.

Desigur că aceste norme sunt supuse permanent verificării prin aplicare practică, analiză doctrinară şi nu în ultimul rând constituţională, toate acestea cu tendinţa de a identifica soluţii şi teze ce ar asigura perfecţiunea şi compatibilitatea acestora cu normele internaţionale ce reglementează acelaşi domeniu.

Referinţe

Antoniu G., „Observaţii la proiectul noului Cod de procedura penală", în *Revista de drept penal*, nr. 1/2009

Botnarii I., „Nomenclatorul, criteriile de clasificare şi categoriile măsurilor speciale de investigaţii", în *Revista Legea şi Viaţa*, Martie 2018

Bradley N., „Evidence, special investigative techniques the right to a fair hearing", în *Revista ERA Forum*, vol.15, nr. 1/2014

Bulancea M., Zlati G., Slăvoiu R., în Udroiu M. (coordonator), *Codul de procedură penală*, Editura C.H. Beck, Bucureşti, 2017

Carlaşuc I., „Regimul extrajudiciar al activităţii operative de investigaţii în realizarea sarcinilor stabilite prin lege", în *Revista Teorii şi practici de guvernări democratice*/Materialele sesiunii de comunicări ştiinţifice 23-24.10.2010

Cobîrşenco I., Fală M., „Principiul proporţionalităţii măsurilor special de investigaţii. Garanţia dreptului la viaţă privată", în *Revista Naţională de Drept*, nr. 12/2017

Copeţchi S., „Provocarea infracţiunii în contextul măsurilor speciale de investigaţii", în *Revista Institutului Naţional al Justiţiei*, Chişinău, nr. 2(41)/2017

Covalciuc I., „Actualitatea şi importanţa activităţii speciale de investigaţii în contextul ultimelor modificări legislative" în *Buletinul Ştiinţific al Universităţii de Stat Bogdan Petriceicu Haşdeu, Ştiinţe sociale* nr. 2(4)/2016

Covalciuc I., „Reflexii asupra evoluţiei istorice a reglementărilor normative privind activităţile speciale de investigaţii", în *Revista Naţională de Drept*, nr. 11/2016

Cuşnir V., *Corupţia. Reglementare de drept, activităţi de prevenire şi combatere. Partea I*, Academia de Poliţie Stefan cel Mare, Chişinău, 1999

Dolea I *et. al.*, *Tratat de drept procesual penal*, Editura Cartier Juridic, Chişinău, 2005, p. 605.

Dolea I., *Drepturile persoanei în probatoriul penal. Concepţia promovării elementului privat*, Editura Cartea Juridică, Chişinău, 2009

Dongoroz V. *et. al.*, *Explicaţii teoretice ale Codului de procedură penală român Partea generală*, Bucureşti, 1975.

Eni A., „Analiza hotărârilor CtEDO adoptate în privinţa Republicii Moldova în materia admisibilităţii tehnicilor de utilizate în operaţiunile sub acoperire în cadrul investigaţiilor penale", în *Revista Studia Universitas Moldaviae*, nr. 8 (118)/2018

Mateuţ G., „Observaţii critice privind noua reglementare a supravegherii tehnice într-o perspectivă comparativă", în *Caiete de Drept Penal*, nr. 3/2015

Mateuţ G., *Procedura penală*, Editura Universul Juridic, Bucureşti, 2019

Mârzac V., Glăvan B., „Utilizarea mijloacelor tehnice în activitatea specială de investigaţii", Academia de Poliţie Ştefan cel Mare, 2014

Moraru V., Covalciuc I., „Particularitaţile exercitării controlului asupra măsurilor speciale de investigaţii autorizate de către procuror", în *Revista Legea şi Viaţa*, nr. 12/2016

Neagu I., *Drept procesual penal. Partea generală*, Bucureşti, 1981

Osoianu T, Orîndaş V., *Procedură penală. Partea generală. Curs universitar*, Chişinău, 2004

Osoianu T., *Reforma judiciară şi de drept în Republica Moldova. Condiţie necesară în vederea integrării europene.* http: //www.ipp.md/old/print.php?l=ro&idc=167&id=495, p.1-2, 15 şi Apud din Мартынчик Е., *Судебная власть в Молдове*, часть первая (историко-правовые очерки), Изд-во ULIM, Chișinău, 1999

Poalelungi M., Dolea I. *et. al.*, *Manualul judecătorului pentru cauze penale*, Chişinău, 2013

Răileanu R.P., „Principiile fundamentale ale procesului penal român în lumina noului cod de procedura penală", în Revista *Dreptul*, nr. 6/2014

Roman D., Popa S., „Identificarea persoanei prin măsuri şi metode speciale de investigaţii", În *Studia Universitatis Moldavie*, Seria ştiinţe juridice nr. 3 (103)/2018

Rusu V., Covalciuc I., „Unele reflecţii asupra sistemului şi conţinutului principiilor activităţii speciale de investigaţii", în *Revista Naţională de Drept*, nr. 8/2015

Udroiu M., *Procedură penală. Partea specială,* ed. 3, Editura C.H. Beck, Bucureşti, 2016

Udroiu M., Slăvoiu R., Predescu O., *Tehnici speciale de investigare în justiţia penală*, Editura C.H. Beck, Bucureşti, 2009

Volonciu N., *Tratat de procedură penală, vol. 2,* Editura Paideia, Bucureşti, 1996