10.53477/2284-9378-21-36

ENSURING LEGAL SECURITY IN THE CONTEXT OF THE EVOLUTION OF CYBER THREATS

Lieutenant-colonel Sorina Ana MANEA*

Ensuring legal security, a primary condition of the rule of law, is nowadays enhanced by the dynamics and complexity of the impact of cyberspace. Although in general, when discussing cyber threats, the issue is approached from the perspective of attacks on network systems and information systems, complex cyber threats can also be generated by the legal system. The collection and processing of personal data is carried out through a process we call Big data, which ensures the conversion of everyday life into a data stream. The result is a new way of social life, based on continuous follow-up and offering unprecedented opportunities for social discrimination and behavioral influence. With this approach we are trying to submit to the debate the guarantee of a climate of stability created by the legal system in the context of cyber threats.

Keywords: legal security; cyber security; defence and national security.

The rule of law is enshrined in Article 1 (5) of the Constitution[1]. The significance of this fundamental concept in practice is that, in addition to the observance of the law by the entire population, state institutions also have the obligation to comply with the law and, of all state institutions, the legislature has the most stringent need to fulfill this obligation in the sense that the legislative activity must be carried out within the limits and in accordance with the fundamental law.

As Parliament is the sole authority with the power to legislate, as a result of the exercise of legislative power, it also has an additional obligation, namely to ensure the quality of the law, as it must be known and understood by its subjects. The need to know and understand the law as a result of its formulation in a clear, precise and predictable manner is the way to comply with the principle of legal certainty from the perspective of its addressees.

Legal certainty as a principle is enshrined in international law, but also in the case of jurisprudence and implies the obligation for the law to ensure its recipients the ability to adapt their behavior with certainty[2] and also to protect legal subjects against arbitrary use of state power[3]. In that regard, the Court of Justice of the European Communities has held that "It must be borne in mind that the principle of the protection of legitimate expectations and the principle of legal certainty form part of the Community legal order and must be respected by the Member States".[4]

The principle of legal security expresses the fact that citizens must be protected against uncertainty and insecurity generated by legal norms and their non-unitary interpretation "against a danger that comes from the law itself, against an insecurity created by law or that it risks creating"[5].

The European Court of Human Rights has emphasized the importance of ensuring the accessibility and predictability of the law, "ruling that "a law" can only be considered a sufficiently precise rule to enable an individual to regulate his or her conduct. The individual must be able to foresee the consequences that may arise from a given act"[6]; "a rule is foreseeable only when it is drafted with sufficient precision, in such a way as to allow any person – who may, if necessary, to seek specialist advice – to correct his conduct"[7]; "in particular, a rule is foreseeable when it offers a certain guarantee against arbitrary infringements of public power."[8]

As a result of enshrining the principle of accessibility and predictability in Community law, and implicitly pursuant to art. 11 of the Constitution, the principle of legitimate expectations was also developed. According to the case law of the Court of Justice of the European Union[9], the principle of the protection of legitimate expectations requires that the legislation be clear and predictable, uniform and coherent and requires that the possibilities for amending legal rules be limited[10].

PhD Student, "CAROL I" National Defence University
e-mail: *sorinaman2@yahoo.com*

Among other things, the principle of legal certainty is closely linked to ensuring the uniform interpretation of the law. In this regard, in the case of Păduraru v. Romania 2005, the European Court of Human Rights ruled that "in the absence of a mechanism to ensure the coherence of the practice of national courts, such profound divergences of jurisprudence, which persist over time and belong to an area great social interest, are likely to give rise to permanent uncertainty (mutatis mutandis, Sovtransav to Holding, cited above, § 97) and to diminish public confidence in the judiciary, which is one of the fundamental components of the rule of law."[11]

Maintaining legal certainty and the trust of the recipients of the law in the legal system is also achieved by establishing guarantees against harm caused by the arbitrary use of public power, such a guarantee being democratic control over the executive authority exercised by the Parliament.

The relevance of the principle of legal certainty as well as of the correlative principles[12] becomes even more evident in the context in which the cyber field is today a vital component of society. So far, Romania does not have a systematic legislation in the field of cybersecurity, which is properly correlated with the legislation in the field of national defense and national security, although the Romanian Constitutional Court has held that cyber security is intrinsically linked to national defense and national security.[13]

Although currently, from the perspective of protecting the infrastructure of information systems, as well as public or private law institutions competent to implement security policies, in the sense of IT protocols to maintain the security of networks and information systems the provisions of Law no. 362/2018 are applicable on ensuring a high common level of security of networks and information systems that fully transposes Directive (EU) 2016/1.148[14] the guarantees offered to citizens against the arbitrary use of state power are difficult to identify.

Thus, the control of the activity of the national authority in the field of security of networks and information systems is performed by the Supreme Council of National Defense[15], in its capacity as organizer and coordinator of activities related to the defense of the country and national security. However, given the constitutional nature of the field of national security, as well as the impact that a possible failure to ensure cyber security may have on national security, the possibility of democratic control through the legislature seems more appropriate.

In the same manner, the Romanian Constitutional Court[16] noted that the European Parliament stated in Amendment 10a) that "taking into account the differences between national governance structures and to maintain existing sectoral mechanisms or Union supervisory and regulatory bodies, Member States should have the power to designate several competent national authorities responsible for carrying out the tasks related to the security of the network and computer systems of the market operators covered by this Directive. However, in order to ensure good cross-border cooperation and communication, it is necessary for each Member State to designate a single point of single contact responsible for cross-border cooperation at Union level, without prejudice to sectoral regulatory mechanisms. Where its constitutional structures or other provisions so require, a Member State should be able to designate a single authority to perform the tasks of the competent authority and the single point of contact. Competent authorities and points of single contact should be civilian bodies, fully functioning on the basis of democratic control, and should not be engaged in intelligence, law enforcement or defense activities, nor should they be organizationally linked in any way with bodies active in these fields. [17]

The European Parliament's comments on the separation of the competent authorities in the field of cyber security and those in the field of information, law enforcement or defense are especially significant in the current context of the debate on the violation of fundamental freedoms by restrictive measures under unequivocal legal rules. In this sense, it is found that, in the last seven years, the Constitutional Court has developed a rich jurisprudence on access, processing and storage by state law enforcement structures to data and information protected by art. 26 and 53 of the Romanian Constitution. This intense process of constitutional control has generated significant changes in the legislation in the field of national defense and national security, which indicates that the legislator did not pay due attention to the

quality of normative acts and therefore we can say that it generated inconsistencies in following the principle of legal security, and especially the principle of legitimate expectations.

Also related to compliance with the principle of legal security are issues related to the processing and storage of traffic data relating to subscribers and users by the provider of a public electronic communications network or by the provider of an electronic communications service intended for the public. Thus, on 6 October 2020, the Court of Justice of the European Union ("CJEU") ruled that the ePrivacy Directive[18] does not allow EU Member States to adopt legislation aimed at restricting the scope of its confidentiality obligations, except if the general principles of EU law, in particular the principle of proportionality, and the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union[19] are respected. The cases before the Court concern the United Kingdom, France and Belgium, whose legislation provided for the obligation for providers of electronic communications services to transmit to public authorities data on the traffic and location of individuals or to keep such data in a general and non-discriminatory manner, such as and storing this data for different time intervals. The reason for such a provision in the legislation of those States was the protection of national security. However, the CJEU has established that such laws fall within the scope of the above-mentioned Directive, noting that: "Although it is up to the Member States to define their essential security interests and the fact that a national measure has been taken to protect national security cannot make EU law ineffective and exempt Member States from their obligation to comply with that law."[20]

The CJEU has set limitations on the ability of Member States to restrict the scope of the Directive, stating: "it must be borne in mind that the protection of the fundamental right to privacy requires […] that derogations and limitations on the protection of personal data must be applied only in so far as they are strictly necessary"[21], the Directive excluding national provisions requiring providers to keep general and non-discriminatory data on trafficking and location as a preventive measure to protect national security and combat crime.

However, the CJEU has also provided for several situations in which Member States may derogate from the general confidentiality requirements of the Directive in order to protect national security, combat serious crime and prevent serious threats to public security, on condition that: it provides for these derogations clearly and precisely; material and procedural requirements are implemented; and the persons concerned have effective safeguards against any abuse. In particular, the CJEU has authorized orders requiring providers to maintain the general and non-discriminatory retention of traffic and location data, as well as targeted storage if a Member State faces a serious threat to national security which proves to be genuine, present or foreseeable, as long as the measure is subject to effective control by an independent court or administrative body disposed of for a period of time deemed strictly necessary.

In Romania, the law stipulates that traffic data relating to subscribers and users stored by the provider of a public electronic communications network or by the provider of an electronic communications service intended for the public, must be deleted or transformed into anonymous data, when they not are still required for the transmission of a communication, but not later than 3 years from the date of the communication[22].

Conclusions

Therefore, the elements on which the principle of legal certainty is based are the certainty and predictability of the law. They are necessary in order to maintain the legitimate confidence of citizens in the legal system and, in the alternative, in the state authorities, whether they are representatives of the legislative, the executive or the judiciary bodies. We consider that the observance of the principle of legal security is a requirement for the protection of social security, a component of national security.

NOTES:

1 *Constitution of Romania*, Monitorul Oficial no. 767 din 31 October 2003.

2 The European Court of Human Rights ruled in the Judgment of 26 April 1979 in the Sunday Times v. The United Kingdom of Great Britain and Northern Ireland, para. 49 that "can be considered as "law" only a norm stated with sufficient precision, to allow the individual to regulate his conduct. The individual must be able to foresee the consequences that may arise from a given act ", meaning that" a rule is foreseeable only when it is drafted with sufficient precision, in such a way as to allow any person – who, if necessary, can resort to specialized advice – to correct their conduct" and when

"it offers a certain guarantee against arbitrary violations of public power." The principle of legal certainty correlates with the principle of legitimate expectations (Cases *Facini Dori v. Recreb Srl*, 1994, available at http: //ier.gov.ro/wp-content/uploads/rezumate-cjue/61992J0091.pdf, last accessed September 2021 and Foto-Frost v. Hauptzollamt Lübeck-Ost, 1987, available at https: //curia.europa. eu / jcms / upload / docs / application / pdf / 2009-05 / tra-doc-ro-arret-c-0314-1985-200802165-05_00.pdf, last accessed September 2021), which requires that the legislation be clear and predictable, unitary and coherent, limiting the possibilities to change the rules raises the stability of the rules established by them.

3 Article 21 of the *Treaty on European Union and Communication from the Commission to the European Parliament, the European Council and the Council COM (2019) 163 final* of 03.03.2019, Further strengthening the rule of law within the Union, Introduction, para. 2, https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52019DC0163&from=EN, last accessed on September 2021.

4 *Case C-381/97*, Belgocodex, para. 26 available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61997CJ0381&from=EN, last accessed on September 2021.

5 Artin Sarchizian, *Principiul securității juridice,* 14.04.2019, available at http://www.drepturile-omului.eu/jurnalul/jurnalul-drepturilor-omului-nr-12019/params/post/1768664/principiul-securitatii-juridice, last accessed on September 2021.

6 *Judgment of the European Court of Human Rights Sunday Times v United Kingdom of Great Britain and Northern Ireland*, 1979, http://hudoc.echr.coe.int/eng?i=001-57584, last accessed on September 2021.

7 *Judgment of the European Court of Human Rights Rotaru v. Romania*, 2000, available at. http://hudoc.echr.coe.int/eng?i=001-58586, last accessed on September 2021.

8 *Judgment of the European Court of Human Rights in Damman v. Switzerland*, 2005, available at http://hudoc.echr.coe.int/eng?i=001-75174, last accessed on 2021.

9 *Judgment of the Court of Justice of the European Union in the case of Faccini Dori v Recreb Srl*, 1994, paragraph 21 et seq., Available at https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri= CELEX: 61992CJ0091 & from = EN # Footnote *, last accessed September 2021; *Foto-Frost v Hauptzollant Lübeck.Ost*, 198722, paragraph 9, available at https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:61985CJ0314&from=EN, last accessed on September 2021.

10 *Judgment of the Court of Justice of the European Union of 24.03.2011*, ISD Polska sp. z o.o. and Others v European Commission, Case C-369/09 P. "Every individual has the right to rely on the principle of the protection of legitimate expectations if he finds himself in a situation where the Community administration, by providing precise assurances, determined it to have good hopes (Case 16/86 Delauche v Commission [1987] ECR I-0000, paragraph 24, Kögler v Court of Justice, Case C-82/98 P . pI-3855, paragraph 33, and Case C-182/03 and C-217/03 Belgium and Forum 187 v Commission [2006] ECR 5479, paragraph 147. In addition, the assurances given must comply with the applicable rules (see, to that effect, Case 228/84 Pauvert v Court of Auditors [1985] ECR I-0000, paragraphs 14 and 15, and Case of 6 February 1986, Vlachou v Court of Auditors, 162/84, Rec., p.481, paragraph 6)", available at https://eur-lex.europa.eu/legal-content/RO/TXT/? uri = CELEX: 62009CJ0369, last accessed on September 2021.

11 *Judgment of the European Court of Human Rights Păduraru v. Romania 2005*, paragraph 99 et seq., Available at http://legislatie.just.ro/Public/DetaliiDocumentAfis/72598, last accessed on September 2021.

12 Supra footnote 2.

13 Decision of the Constitutional Court no. 455/2018 regarding the admission of the objection of unconstitutionality of the provisions of the Law on ensuring a high common level of security of computer networks and systems and the Decision of the Constitutional Court no. 17/2015 on the admission of the objection of unconstitutionality of the provisions of the Law on cyber security of Romania.

14 *Directive (EU) of the European Parliament and of the Council 2016 / 1.148 of 6 July 2016 on measures for a high common level of security of networks and information systems in the Union*, published in the Official Journal of the European Union, L series, no. 194 of July 19, 2016.

15 *Government Decision no. 494 of May 11, 2011 on the establishment of the National Cyber Security Incident Response Center - CERT-RO.*

16 *Decision of the Constitutional Court no. 17/2015 on the admission of the objection of unconstitutionality of the provisions of the Law on cyber security of Romania.*

17 *Report: PE 514.882v02-00 of 12.02.2014 on the proposal for a directive of the European Parliament and of the Council on measures to ensure a high common level of network and information security in the Union (COM (2013) 0048 - C7-0035 / 2013 - 2013/0027 (COD)* available at https://www.europarl.europa.eu/doceo/document/A-7-2014-0103_EN.html?redirect, last accessed on 02.02.2021

18 *Article 15 (1) of Directive 2002/58 / EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the public communications sector (Directive on confidentiality and electronic communications), as amended by Directive 2009/136 / EC of the European Parliament and of the Council of 25 November 2009*, available at https://www.dataprotection.ro/servlet/ViewDocument?id=201, last accessed September 2021.

19 https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:12012P/TXT&from=DE, last accessed on September 2021.

20 Available at http://curia.europa.eu/juris/document/document_print.jsf?docid=232084&text=&dir=&doclang=RO&part=1&occ=first&mode=DOC&pageIndex=0&cid=5875047#Footnote*, accessed on 03.02.2021.

21 *Judgment of the Court of Justice of the EU (Second Chamber), 14 February 2019 on the processing of personal data* - Directive 95/46 / EC - Article 3 - Scope - Video recording of police officers inside a police station during performance of procedural acts - Publication of video recordings on a website - Article 9 - Processing of personal data only for journalistic purposes - Notion - Freedom of expression - Protection of privacy, para.64, available at https:

// curia .europa.eu / juris / document / document_print.jsf? docid = 210766 & text = & dir = & doclang = RO & part = 1 & occ = first & mode = req & pageIndex = 0 & cid = 14089710, last accessed on 03.02.2021.

22 Art. 5 of *Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, as subsequently amended and supplemented*.

REFERENCES

Constantinescu, Mihai; Iorgovan, Antonie; Muraru, Ioan; Tănăsescu, E.S., *Constituția României revizuită – comentarii și explicații,* Editura All Beck, București, 2004.

Dima, B., *Conflictul între palate. Raporturile de putere dintre Parlament, Guvern și Președinte în Rmânia post comunistă,* Editura Hamangiu, București, 2014.

Duțu, P., Sarcinschi, A., & Bogzeanu, A., *Apărarea Națională, între viziune și realitate, la început de mileniu,* Editura Universității Naționale de Apărare „Carol I", București, 2013.

Iorgovan, A., *Tratat de drept administrativ* , vol. 2, Editura Nemira, București, 1996.

Mâță, D. C., *Securitatea națională - concept, reglementare, mijloace de ocrotire,* Editura Hamangiu, București, 2016.

Moțiu, E. I., *Autoritățile administrative autonome din domeniul siuranței naționale și al mediatizării informațiilor,* Editura C.H. Beck, București, 2010.

Muraru, I., *Drept Constituțional și Instituții Politice,* Editura Actami, București, 1998.

Panc, D., *Securitatea cibernetică la nivel național și internațional. Instrumente normative și instituționale,* Editura Hamangiu, București, 2017.

Predescu, I., & Safta, M. (fără an). *Principiul securității juridice, fundament al statului de drept. Repere jurisprudențiale*. Disponibil la https://www.ccr.ro/wp-content/uploads/2021/01/predescu.pdf.