OPINIONS ON THE UNCONSTITUTIONALITY ASPECTS RELATED TO THE CYBERSECURITY LAW

Maxim DOBRINOIU[*]

Abstract

Nowadays, on a rise of Cybersecurity incidents, with even more ferocious and sophisticated methods and tools of performing online attacks, the governments should struggle to create effective counter-measures, both in terms of technical endeavours and strong legal provisions. Following a successful Cybersecurity Strategy, the Romanian government's Cybersecurity Law proposal was expected to bring the much needed safety measures in the national component of the cyberspace, but was dropped for unconstitutional reasons, reopening the debate on national security versus the protection of citizens' constitutional rights to privacy.

Keywords: *Cybersecurity, cyber-attacks, cyber-infrastructures, national security, privacy, personal data, constitutional rights.*

1. Introduction

In a very complex virtual environment, Romania is one of the few European countries that drafted and put in place a good and comprehensive Cybersecurity Strategy[1], assumed and endorsed, at the time of its creation, by state authorities, private IT&C companies and various non-governmental organizations. All of them agreed on the necessity of the existence of such a strategy, as a first legal commitment towards assuring the security of the national component of the cyberspace (Internet) and the protection of networks and information (critical) infrastructures against the high level threats posed by cyber-offenders, criminal organized groups, cyber-terrorists, and even state(sponsored)-entities.

2. The Cybersecurity Law - CSL

In pursuing the guidelines and main ideas of the Strategy, the Romanian government issued, by the end of year 2014, a draft Cybersecurity Law that was adopted by the Parliament as the first legislative bill of its kind.[2]

But, the Cybersecurity Law did not have the chance to come into force, due to a broad wave of criticism from various NGOs, social media and citizens, being even disproved by 69 members of Parliament in a legal appeal to the Constitutional Court based on assumptions of unconstitutionality of the provisions, interference with the constitutional rights of people and lack of realistic safeguards to protect personal data and privacy against the security-based operations run by the competent state authorities.

The Cybersecurity Law was created with the aim to establish the general framework for regulation in the Cybersecurity area, with the obligations for the legal persons, with both public and private liability, to protect the cyber-infrastructures they own, hold, operate or use. CSL also provided the concept of "Cybersecurity" as a component of national security that can be, basically, realized through acknowledgement, prevention and countering the threats and attacks in cyberspace, as well as through reducing the vulnerabilities of the cyber-infrastructures, in order to mitigate the risks to their security.

3. The Criticism formulated by the Constitutional Court

One of the first accusations brought to CSL was the lack of harmonization with the well-known and much-discussed European Directive concerning measures to ensure a high common level of network and information security across the Union (known as the Network and Information Security Directive or NIS Directive)[3].

But this bill has not yet been adopted and has no effect on the Member States national legislations, with serious doubts regarding its final form.

For this, we appreciate as questionable the manner in which the Constitutional Court of Romania – CCR was quick to highlight, within its decision upon the unconstitutionality of the CSL, that the "competent authorities" and the single contact points in the area of Cybersecurity should only be "civilian bodies",

[*] PhD, Faculty of Law, "Nicolae Titulescu" University of Bucharest (e-mail: **office@e-crime.ro**).

[1] Approved by Government Decision no.271/2013, published in the Official Gazette no.296/23.05.2013

[2] The Cybersecurity Law bill was adopted by the Romanian Senate, as decisional chamber, on 19.12.2014, and was further sent to promulgation to the President of Romania. Meantime, the bill was contested to the Constitutional Court of Romania by 69 deputies and various NGOs.

[3] Legislative initiative of the European Commission, unfinished and currently still on debate (in the first reading) in the European Parliament, where has been adopted with modifications on 13.03.2014. On this form, the CE only expressed a partial approval

"subject of full democratic oversight", that "should not fulfil any intelligence, public safety or defence-led activities", and, moreover, that "should not be linked in any organizational way with any institutions of this kind" – as provided by Article 6 of the proposed NIS Directive.

In this way, CCR threw a doubt shadow on the defence, public safety and national security institutions, including in terms of the democratic control of their activity, issue that was not quite appropriate to be analyzed in that Decision.

Another problem of the CSL was the scope of the bill. In the section named "definitions", the CSL provided the explanations for two expressions, namely "cyber-infrastructure" and "cyber-infrastructure of national interest" – CINI, that were, then, balanced among different provisions (articles), with a high contribution towards the creation of a feeling of unpredictability and lack of clarity to those legal persons CSL should have applied to.

In this context, we consider that CSL should have been more accurate, more explicit, and should have restricted its scope only to those infrastructures that are essential for maintaining the vital economic and societal activities in the field of energy, transports, financial services, telecommunications and information society, food and health supply chains, and also in defence, public order and national security, whose disruption and destruction of might have a significant impact within a EU Member State (as also provided by Article 3 of the proposed NIS Directive). With other words, a new CSL should address just the protection of cyber-infrastructures of national interest, because only this activity could be comprised into the general concept of *national security*.[4]

The CCR support for the idea of a "civil body" as a national authority in Cybersecurity seems to have the origins only in the NIS Directive project, and less in the realities of the cyberspace, where, daily, show up new forms of menace against citizens (users), businesses and even states, and the protection of essential cyber-infrastructures has become a real component of national security.

Also surprisingly, the Constitutional Court placed in a certain doubt the principles of legality based on which the defence, public order and national security institutions guide their activities (principles that are comprised in their specific law of organization and functioning), assigning them the unreal intention to use CSL to collect intelligence through infringement of constitutional rights to personal, family and private life and the confidentiality of correspondence, even if CSL was only meant to legal persons with both private or public liability[5].

In the same logical stream, the CCR could even deny the legality of the electronic communications' interceptions performed by the National Technical Centre – a military structure within the Romanian Intelligence Service, nowadays the only legal authority in the area of electronic eavesdropping, on the same grounds of "not being reliable" or "being a threat to the constitutional rights to personal, family and private life, or the confidentiality of communications.

So, it is not very clear if CCR objected against the "military structure" of the competent authorities mentioned by the CSL or just acknowledged their lack of generic legal powers or the absence of the necessary safeguards for the protection of constitutional rights to privacy and confidentiality of communications. CCR's idea may very well be appreciated as a dangerous turning point for the legal base of those authorities, with possible repercussions on their further operations in cyberspace.

Far from other aspects, one of the most controversial issues identified by the CCR on CSL was "the access to the data held by the holders of cyber-infrastructures", while the constitutional court suggested a double-analysis: one from the perspective of the *type of data* to which the access is granted, and the second one from the perspective of *the way the access is fulfilled*.

In the first hypothesis, CCR considered that, although CSL bill has not provided for, the access to the data held by the persons subject to the law does not exclude the access to, the processing or the usage of personal data.[6] This opinion is relevant and fair, and we fully agree with it. Yes, technically, it is possible that among all the data stored about security incidents or cyber-attacks to also be found information related to a natural person. But, CCR forced the interpretation of CSL, pointing-out that "it is obvious that the type of data contained in these systems and networks include data relating to private life of the users", and that "the authorities designated by the law must be allowed an access to any data stored on these cyber-infrastructures", thus "a discretionary access also to data related to private life of the users".

This CCR observation is also correct. The new CSL bill should adopt a much clearer provision on the data on security incidents or cyber-attacks that the cyber-infrastructure holders need to retain/record, and what is the data they may disseminate/communicate to the competent authorities. Content of messages or other data related to a person's private communication should not be processed whatsoever.

From another point of view, based on the logic of the CCR's opinion, one could very well interpret that the persons subject to CSL usually store or hold personal data on their systems. This means that either those persons are *personal data operators* and comply

[4] Currently, in what regards the protection of the critical information infrastructures, there is in force the Government Emergency Ordinance no.98/2010, published in the Official Gazette no.757, part I, of 12.11.2010, and approved by Law no.18/2011

[5] Paragraph 51 of the Decision no.17/2015 of the Romanian Constitutional Court

[6] Paragraph 59 of the Decision no.17/2015 of the Romanian Constitutional Court

with the legal provisions of Law no.677/2001[7], or they are providers of electronic commerce services and comply with the provisions of Law no.365/2002[8]. But, in both situations, whatever motivation the competent authorities may invoke for their data requests, any eventual personal data could be easily refused by the holders of cyber-infrastructures for the reason of no consent from the natural person who actually owns that data.

In Paragraph 62 of its Decision, CCR put the sign equal between the terms "access to data concerning a cyber-infrastructure" (in CSL) and "access to a computer system" – as provided for by Article 138 Para 1 point b) and Para 3 of the Criminal Procedure Code. The latter is defined by the Code as "entering a computer system or a computer data storage medium, either directly or remotely through specialized software or through a network, in order to identify evidence". According to the Criminal Procedure Code, this legal measure could only be ordered by a judge (under Article 140) or a prosecutor, for 48 hours (under Article 141).

This idea of "equality" between the two terms is at least questionable; it seems that CCR did not take into consideration the technical aspects comprised in the phrase "entering a computer system or a computer data storage medium", as intrusive acts which do not have anything in common with making available or communicating data – as activities fulfilled by the holder of cyber-infrastructures following the requests from the competent authorities (see CSL).

The second aspect related to "data access", criticized by CCR, refers to the lack of a regulation on the ways the competent authorities effectively realize the access to the data stored by the holder of cyber-infrastructures, and also refers to the lack of any objective criteria to restrict/limit to the minimum the number of employees that may have access to or could further use that data, and especially refers to the absence of a prior control from a court of justice. All these aspects were seen by CCR as "an interference with the fundamental rights to personal, family and private life, and the confidentiality of correspondence".[9]

We consider this CCR opinion as insufficiently substantiated, because, again, it does not reflect at all the technical realities of the cyberspace, not the judicial practice. The IT specialists know that not just any security incident or any cyber-attack (as they have been defined by CSL) is automatically an offence for which a criminal prosecution may begin, *in rem* or *in personam*.

Usually, for the investigation of the causes that determined such events related to a cyber-infrastructure, gathering relevant information may not be subject of a judicial control or of a formal approval from a prosecutor or a judge. In the majority of such cases, administrative measures are sufficient. But this should apply strictly for technical data necessary in a Cybersecurity investigation of the reported event.

In all security incidents or cyber-attacks cases, the most important for the investigation is the information generated by the event, computer data that may lead to relevant conclusions on the source of the incident, means of exploiting vulnerabilities, possible real targets and future developments. The bad feature of this kind of data is its volatility – data could be easily lost, altered, modified or deleted, accidentally or on purpose, automatically or due to human intervention/error.

A possible legal solution able to meet both CCR requirements and the technical needs for reliable computer data (for investigation), would be a specific and clear provision in the new CSL, that may offer the competent authorities the power to order (by an administrative act/request) the holder of a cyber-infrastructure to expeditiously preserve stored computer data in connection with a security incident or a cyber-attack, following the model of Article 154 of the Criminal Procedure Code. And only then, based on an authorization issued by a judge of freedoms and liberties, would further be possible the access to the respective data. In such way, the authorities could be able to obtain unaltered data relevant in the context of their investigations, in conditions of full safeguarding the protection of constitutional rights of individuals.

In what regards CCR observations on the subject of "cyber-infrastructures of national interest", we fully agree with the ideas comprised in Paragraphs 71 and 73 of the Decision.

Another controversial issue, insufficiently approached, neither in doctrine, nor in judicial practice, is CCR joining the opinion that "IP addresses are personal data", meaning that are data by which a natural person is identified or identifiable (as specified by Law no.677/2001).[10]

Similar ideas have been circulated in the EU[11], and among local non-governmental organizations active in the area of privacy in IT&C, and are in compliance with certain points of view expressed by the European Court of Justice on specific cases[12].

We consider such conclusion as an error of interpretation, at least from the following considerations:

a) An IP address is just a simple technical information, based on which the relevant protocol[13] routes data packets in a network (internet);

[7] Law on the protection of persons regarding the processing of their personal data and for the free circulation of such data
[8] Law on electronic commerce
[9] Paragraph 63 of the Decision no.17/2015 of the Romanian Constitutional Court
[10] Paragraph 75 of Decision no.17 of 2015 of the Romanian Constitutional Court
[11] https://www.huntonprivacyblog.com/2014/11/articles/german-court-asks-european-court-justice-ip-addresses-personal-data/
[12] See European Court of Justice Decision in case no. C-70/10 Scarlet Extended vs. SABAM
[13] Transmission Control Protocol

b) In the absence of other relevant information, an IP address is not able to effectively identify a natural person;

c) An IP address only points to connected electronic devices or equipment, active or passive network elements, internet resources, but not the users;

d) An IP address is similar to a cellular number provided by a Prepay SIM card: it cannot offer significant elements based on which a natural person to be identified (could be, somehow, possible but only in connection with other data). Therefore, neither a cellular number provided by a Prepay SIM card may be regarded as "personal data";

e) An IP address is similar to a vehicle registration number, when the vehicle belongs to a legal person (institution, organization, company etc.) and is registered on its name. Therefore, neither a vehicle registration number may be automatically considered as "personal data".

In logic theory, if a given situation (p) implies another situation (q), then the second situation denied (non q) implies the first situation denied (non p). Applying this theory formula to the definition of "personal data" as it is in the specific law, we come to the conclusion that:

if ("the information is personal data") -> ("the information is able to identify a natural person"), then ("the information is not able to identify a natural person") -> ("the information is not personal data"). In other words, if an IP address is not able, by itself, to identify a natural person, then that IP address is not a personal data.

Last but not least, in Paragraph 89, CCR raised up critics on a certain provision of CSL concerning the right of the representatives of the competent authorities "to request statements or any document needed in order to carry out the control, to conduct inspections, even unannounced inspections, at any facilities, premises or infrastructures intended for national interest".

In CCR's opinion, the permission to conduct inspection granted to the representatives of the competent authorities requires access to a specific location, with respect to certain objects, computer systems for data storage, processing and transmission of data, including personal data, access that call into question the protection of the users' constitutional rights, with no safeguards provided by CSL against the risks of abuse.

Moreover, surprisingly, CCR regards the term "facility" (mentioned in Article 27 Para 2 point b.) as "a computer system or a network or an electronic communications service, while "the access to them would not be permitted without an authorization from a judge". In such case, especially when dealing with *premises*, CCR considered that would be applicable the provisions of Articles 157-167 of the Criminal Procedure Code related to *home search and seizure* activity, measure ordered only by a judge.

CCR observations seem to be correct, but, once again, they simply ignore specific realities: no one can eliminate *a priori* the possibility for an authority to conduct a control in the field of a certain activity. In other words, any of the competent authorities mentioned by CSL may perform the controls provided by the law, but only in what regards the security (physical, logical, procedural) of the objectives, facilities or infrastructure-based elements.

CCR wrongfully considers that by "facility" one may understand a "computer system or network". CSL only defines the "cyber-infrastructure", in the details of which could be found the term "computer system". In the view of CSL, the facility refers to a building element, which acts as a shelter (location) for the respective cyber-infrastructures, and this kind of element may be very well be inspected, controlled from its security perspective, even without prior announcement.

In what regards the "premises" CCR refers to in its Decision, the constitutional court missed the fact that, currently, in real life there are numerous situations when various state authorities (both central or local) are empowered by different laws to conduct controls (announced or not) in premises, without any authorization issued by a judge and even without to consider these activities as "home search and seizure" operations. For example, the controls and inquiries performed by the public health authorities in restaurants, the controls of the National Authority for Consumer Protection in commercial places or businesses, the controls of the State Inspection for Constructions in the premises where there are suspicions related to building activities with no clearance or approval or the controls of the emergency situations inspectorates on fire prevention in all the places where this kind of events may occur.

4. Final remarks

The conclusions and opinions formulated by the Romanian Constitutional Court in the case of Cybersecurity Law, by Decision no.17/2015, constitute a strong incentive for the creation of a better legislation in the field of protecting the national component of cyberspace and the critical information infrastructures against the threats posed by bad individuals or other interested state or private entities, local or foreign.

The present study only brings some technical and legal observations on the analyzed subject, with the aim to contribute to a good understanding of the mixture between legislation and the technical realities of the cyberspace, and to the creation and adoption of a strong new Cybersecurity Law, as a perfect guide for public and private organizations to contribute to the general safety of our nation's cyber-infrastructures.

References

- Decision no.17/2015 of the Romanian Constitutional Court, available at https://www.ccr.ro/files/products/Decizie_17_2015_EN_final.pdf
- Cybersecurity Law bill, available at http://www.cdep.ro/proiecte/2014/200/60/3/pl263.pdf