

RECENT DEVELOPMENTS AS REGARDS CYBERCRIME LEGISLATION IN ROMANIA¹

1. What is the current framework?

Romania has ratified the Council of Europe Cybercrime since 2004 and the internal provisions that correspond to the Convention are to be found in a special law, namely Law 161/2003, Title III on preventing and combating of cybercrime. Of course, to this special framework have to be added the general norms prescribed by the Romanian Criminal Code and Criminal Procedural Code and several special laws that are incident in the field.

The structure of Law 161/2003² clearly shows that the Romanian legislator has followed in quite an accurate way the structure of the Council of Europe Convention by including substantial law and procedural law aspects³, as well as norms dealing with the international judicial cooperation in the field.

The current Romanian cybercrime legislation has proved in the last six years an efficient tool used by the judiciary in order to bring cybercriminals to justice. This special law allowed not only an enhanced activity of the judiciary at internal level, but also an improved cooperation with other countries in the field, faster responses and more effective actions against this truly transnational phenomenon. The quite consistent caseload Romania has covers a wide range of cybercrimes from computer-related fraud and forgery which are the most numerous⁴, to illegal access, data and system interference, misuse of devices or child pornography through computer systems.

The last years have shown an increase of computer crimes committed in an organized manner. The cases of individuals committing illegal access although present are clearly outnumbered by those committed by highly organized groups, concentrating mostly on fake on line auctions, phishing and pharming techniques as well as on credit card offences.

The transnational character is of cybercrime brings a series of challenges to law enforcement agencies that cannot be met in traditional crimes. In this context, the international judicial cooperation⁵ becomes essential in securing and producing the evidence that can assure the success of investigators against cybercriminals.

1 The opinions expressed here belong entirely to the author of this text and do not reflect the official position of the Romanian Ministry of Justice

2 See for details as regards Law 161/2003 and other relevant provisions the country profile available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Romania%20_April%202008_.pdf

3 See for a detailed analysis of the provisions of Law 161 and the way the Convention has been implemented as well as examples of good practices in. Picotti, Salvadori, *National legislation implementing the Convention on Cybercrime.: Comparative analysis and good practices* at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567%20study2-d-version8%20provisional%20_12%20march%2008_en.pdf

4 See for relevant caseload in the field the DIICOT Annual Report 2008 available at <http://www.diicot.ro/pdf/2009/raport2008.pdf> as well as the DIICOT Annual Report 2009 available at <http://www.diicot.ro/pdf/2010/raport2009.pdf>

5 See for examples of good practices Romania has in the matter of international judicial cooperation in cybercrime cases. Pedro Verdelho, *The effectiveness of international judicial cooperation against cybercrime: examples of good practices.* available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567%20study4-Version7%20provisional%20_12%20March%2008_en.pdf See also for caseload Romania has in the matter of MLA in computer crime cases http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/T-CY%20-%20PC-OC%20_2008_%2008%20Computer%20Related%20cases%20FINAL.pdf

2. What does the future bring?

Romania is currently undertaking a significant legislative reform covering the criminal and civil field altogether. In the second half of 2009 a new Criminal Code⁶ has been adopted and by it new changes in the criminal justice system have been brought. It has to be underlined that the new Criminal Code is not in force yet, a law for the practical application of the code being currently under development. The provisional law measures shall be taken over by the new Criminal Procedural Code which is currently under debate in Parliament⁷.

In the following lines we will present briefly only the main changes brought to the substantial law provisions by the new Criminal Code.

a. Cybercrime in general

As previously said, the current legislative framework covering the substantial law provisions is to be found in Law 161/2003 when speaking about the offences stipulated by art. 2 to 9 of the Council of Europe Cybercrime Convention and Law 8/1996 with regard to the offences related to infringement of copyright and related rights enshrined in art. 10 of the same Convention.

The new Criminal Code incorporates the C.I.A offences under Chapter 6 of the new Criminal Code, from art. 360 to art. 366, and the computer related offences and content related offences in different other chapters of the Code, as it will be shown later on. All the offences against confidentiality, integrity and availability of computer data and systems established by the Budapest Convention are to be found in the new Criminal Code (illegal access, illegal interception, data interference, system interference and misuse of device).

The changes brought by the legislator are rather small and consist mainly (but not exclusively) in mitigated punishments compared with the legislation in force, namely Law 161/2003. It has to be said that the issue of mitigated punishments was a general trend of the new Criminal Code as the old one, dating from the late 60s, has promoted, in the opinion of many experts, very harsh punishments which was somehow contradicting with the European standards in the field.

In any case, the slight modifications that have been operated were considered in order to improve the existing legal framework and to leave aside any possible misinterpretations of these legal norms. Such as example is represented by the illegal access in the form committed through infringement of security measures. Art. 51 paragraph 3 of Law 161/2003 which is the provision into force as we speak does mention only infringement of security measures, while art. 360 paragraph 3 of the new Criminal Code explains as well what security measures means, referring to procedures, devices or specialized programs that are restricting or forbidding the access for certain category of users.

Computer related forgery is incriminated by art. 325 of Title 2 of the new Criminal Code. The main elements of the offence remain the same with one exception, the minimum and maximum limit of the penalty which are mitigated.

Computer related fraud is stipulated by art. 249 of Chapter IV and takes over the current provisions, with the same comment as before regarding the quantum of the punishment.

b. Sexual exploitation of children on the Internet

Art. 9 of the Cybercrime Convention incriminating child pornography committed on line has already been implemented in the Romanian legislation through art. 51 of Law 161/2003. All the modalities stipulated by

6 The new Criminal Code has been published in the Official Gazette no. 510 published on the 24th of July 2009

7 The project of the Criminal Procedural Code in Romanian language can be found at http://www.just.ro/Sections/PrimaPagina_MeniuDreapta/noulcodeprocedurapenala/tabid/941/Default.aspx

the Convention were taken over by the Romanian legislation.

As regards the particular aspect, it has to be said that Romania is currently in the process of ratification of the *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote 2007*. Regulations implementing the Convention have already been introduced in the new Criminal Code.

Important from the perspective of the fight against the on line sexual exploitation of children are the provisions of art. 20 letter f) of the Convention and art. 23-Solicitation of children for sexual purposes or the so-called grooming.

These provisions do not have correspondent in the current legislation and that is why they have been implemented in the new Romanian Criminal Code in art. 374 (Child pornography) paragraph 4 which incriminates the unlawful access of pornographic materials through computer systems and art. 222 (Recruiting minors for sexual purposes).

With reference to the last offence, it has to be mentioned the fact that the age of the minor has to be under 13. The solicitation of the child is made with the purposes to commit a sexual act with that minor or to commit other acts of sexual nature with a minor, including acts committed with the purpose of producing pornographic materials.

3. Conclusions

The new Criminal Code manages to bring together regulations that at the moment are comprised in different special laws, which will present a clear practical advantage. It also brings some new elements that align the Romanian legislation to the standards imposed by the *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* with regard to the sexual exploitation of children on line. How it will be actually applied by the practitioners it remains to be seen after its entrance into force.

For now suffice it to say that Romania has the adequate legislative framework, corresponding to the standards imposed by the *Council of Europe Cybercrime Convention* and *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*. This represents the key element in designing valid policies in the field, in order to get the right responses in the fight against this type of criminality.