CONSIDERATIONS ON THE EFFICIENCY OF THE ROMANIAN NEW CRIMINAL CODE IN COMBATTING CYBERCRIME

MAXIM DOBRINOIU[*]

Abstract
The New Criminal Code addresses in an adequate way the challenges of the cyberspace, being a useful tool in the hands of law enforcement agencies involved in combating a large spectrum of communications and cyber-related offences. From a broad perspective, one could state that the changes made to the previous legislation are pertinent considering the real need of indictment outlined by the analysis of the judicial practice, while the new issues essentially contribute to the creation of a modern legal framework, capable of safeguarding the social values which will come up in the near future from the interaction of people with a booming information technology.

Keywords*: crime, computer system, computer data, illegal access, intercepting, computer-related forgery, computer-related fraud, child pornography, harassment, electronic vote, electronic payment instrument*

In what regards the crimes committed with the help or against computer and telecommunications systems, computer data or electronic payment instruments, the Romanian New Criminal Code preserves, in a considerable percentage and with certain „corrections", the provisions of the previous special legal acts (such as the 3rd Title – preventing and combatting cybercrime – from the Law no. 161/2003 – which, at the time, almost literally transposed the 2001 Budapest Council of Europe Convention on Cybercrime into Romanian national legislation, or the Law no. 365/2002 on electronic commerce), but also brought forward new elements, trying to provide legal solutions to certain facts or situations happened in real life (the local judicial practice).

Generally, the New Criminal Code groups in a natural way the computer-related crimes based on the traditional social values, which still need to be protected by criminal provisions, introduces new concepts (e.g. „theft with the purpose of use", „harassment", „fraud to electronic vote" etc.), reformulates relevant articles from the respective special laws, and modifies, in a way of decreasing, the quantum of the imprisonment time. On the other hand, the Romanian legislator inexplicable disposed of the definition of certain terms and expressions, although uses them in the legal texts and, moreover, and don't yet succeed to fully cover the situations, scenarios or cases which quite often occur in cyberspace.

Relevant aspects from the General Part of the Criminal Code

One could remark the definition of the *electronic payment instrument* (Article 180), with the legal text not modified from the previous one - from the Law no.365/2002 on the electronic commerce or from the Romanian National Bank Regulation no. 6 of 2006.

Also, by Article 181 one could find explained the concepts of *computer system* and *computer data*, while the texts are pretty much similar with those provided by the prior Article 35 of the 3rd Title of Law no. 161/2003. Compared to the above mentioned special law, the are no longer available the definitions of *automatic data processing* and *computer program*, elements which could have contributed to a better understanding of the computer systems functioning in the respective criminal context.

Surprisingly, there is missing a very important definition (currently existing within Law no. 161/2003), namely the phrase *without right* (or *illegal*). Most probably, this time the legislator's opinion was that the definition would be no longer needed, but, without providing instead any other explanation regarding the *illegitimate* conditions of the interaction between users/individuals and

[*] Lecturer, PhD in Cybercrime, Faculty of Law, "Nicolae Titulescu" University (email: office@e-crime.ro).

various elements of the virtual environment, there will be somehow difficult for prosecuting authorities to bring correct legal charges (indictments) and to request sentences in strict accordance with the real social threat.

In this context, the actors fighting cybercrime should use (and even understand) the concept of „illegal" at least in the light of the European legislators, as contained in the Explanatory Report of the CoE[1] Convention on Cybercrime, as any behaviour/act/action undertaken with no authority or without permission, irrespective if that permission is granted in a legal, executive, administrative, judicial, contractual or consensual form, and any behaviour/act/action which does not represent, according to the Code, a cause which eliminates its criminal nature.

Relevant aspects from the Special Part of the Criminal Code

By Article 208, the new Code introduces, for the first time in its existence, the crime of *harassment*, incriminating and punishing the making of phone calls or other communications by means of remote transmissions, which, by frequency or content, cause a fear to a person.

The provision comes happily to assist the prosecuting authorities which were confronted, in the past, and still have to face numerous cases like this in practice. By its form, the legal text succeed to cover most of the situations that could affect the right of a person to live his life in privacy (even when this person is present in cyberspace), without interferences or fear. Here, we are talking about defamation or making a sort of psychological pressure on webpages, forums, online chat rooms/groups, the creation of fake accounts in social media or hijacking the real account of an individual, transmitting large amounts of emails or instant messages (internet relay chat), posting defamatory messages on blogs, Facebook, Twitter or other social media, in order to achieve an „informational assault" on the victim or with the aim to produce her fear, anxiety, discomfort etc. Other methods may include the sign up of fake email accounts, by unauthorized or abusive takeover of the victim's identity, followed by sending email messages on behalf of the victim in order to discredit, defame, denigrate, undermine or intimidate her, the creation of fake profiles (by the use of real personal data and photos of the victim) on pornographic, online dating or sexual minorities' websites or blogs, so that the victim is shown in „hard-to-believe" situations or not-compliant with her real social status.

The *online harassment* concept also consists of other material acts, such as: monitoring the victim's online activity, by using electronic surveillance devices or spy-type applications, connecting to the victim's Wi-Fi router and performing illegal online activities (child pornography, computer-related fraud, even hacking), in order to intentionally mislead the authorities to wrongfully bring charges on her etc., but all of these acts can be indicted in a proper way using other legal provisions from the Criminal Code.

In other foreign legislations (ex. US, Canada etc.), but also in the specialized literature, this crime is known and referred to as: Cyberharassment, Cyberstalking or Cyberbullying.

Besides the major benefits in socio-economic environment, the new technologies also brought large number of judicial problems, one of them being the connection to public electronic communications networks or obtaining access to publicly available electronic communications services.

For that, the Romanian legislator created a distinct criminal rule, with no prior correspondent, namely *theft with the purpose of use* (Article 230 paragraph 2), which incriminates the unauthorized use of someone else's communications device or the use of a communications device illegally connected to a network, causing a loss of property. This new legal provision comes to solve controversial situations from real life or doctrine, chiefly regarding the „illegal" connections to communications networks or even to Internet using wireless-enabled electronic devices (IEEE 802.11 standard).

[1] Abbreviation: Council of Europe.

Another win resulted from this new legal text is bringing into the illicit context the situation of using someone else's communications device, while considering that, nowadays, due to technological developments, by *communications device* one could easily see a smartphone or even a personal computer, and most of the so called *voice or video communications* are now entirely based on the IP[2] technology and transmission protocol.

Computer-related fraud (Article 249) preserves almost entirely its original legal text (as in Article 49 of Law no. 161/2003) and now is placed in the large context of the „traditional" crimes against the property, but in a distinct section (Chapter IV – frauds committed by computer systems or electronic payment instruments). Compared to the previous special law, the imprisonment time was reduced (general trend), as from 3 to 12 years (in Law no.161/2003), to 2 to 7 years (in the new Criminal Code).

Same comments and notes shall apply also for the newly-shaped crime of *performing financial operations fraudulently* (Article 250), with the sole mention that the prior legal provision (Article 27 of Law no. 365/2002 on electronic commerce) contained a distinct paragraph incriminating the behaviour of the person which, according to his contractual or employment duties, conducts technical activities for producing and issuing electronic payment instruments (e.g. credit cards) or for performing specific financial operations, has access to the security measures applied to the fabrication of such instruments or has access to personal data or other security mechanisms required for performing specific financial operations, according to the law. The reasons for eliminating the above mentioned legal situations from the new Criminal Code are still unknown, and the new legal text punishes now the employee or contractual agent of credit card or financial institutions with the same imprisonment time as for the other culprits.

The *acceptance of fraudulently performed financial operations* (Article 251) represents an identical version of Article 28 of Law no.365/2002, the only difference being the decreasing of the imprisonment period (from 1 to 12 years - in Law no.365/2002 – to 1 to 5 years – in the new Criminal Code).

The privacy in the sector of electronic communications has also been protected by the new Criminal Code, where the legal provision of *violation of the secrecy of correspondence* suffers only minor changes from previous form (Article 195 of actual Criminal Code). The only aspect that draws attention is the legislator's decision to renounce to the aggravated situation when the incriminated actions are performed by an employee or official who has the legal obligation to preserve the professional secret and the confidentiality of the information he got in touch with or he got access to. In the case of the 2nd paragraph of Article 302, the crime of the *interception, without right, of a conversation or of any communication made by phone or by any mean of electronic communications* is likely to be committed in ideal concurrence with the crime of *interception, without right, of a non-public transmission of computer data* (as referred to in Article 361 paragraph 1 of the new Criminal Code), while the conversation or the communication takes place, from a technical point of view, through computer programs or *Voice over Internet Protocol (VoIP)*-type applications, a technology wide spread and largely used nowadays.

One of the most highly visible crime in the local mass-media, namely *forgery of the electronic payment instruments*, could also be found in the new Criminal Code, in the 2nd paragraph of the Article 311, along with the other „traditional" forgery-related crimes. Compared to the previous version (Article 24 of Law no. 365/2002), one could note the decreasing of the imprisonment period (the maximum of the prison punishment reduced from 12 years to 10 years), as well as the elimination of the aggravated situation when the act of forgery is committed by the employee or the contract agent of the financial or credit institution who's task is to conduct technical operations to issue electronic payment instruments or has access to personal (identification) data or to the security mechanisms associated to the respective electronic payment instruments.

[2] Internet Protocol.

Putting into circulation counterfeit values is a another crime which strengthens the gallery of forgery-related crimes committed against financial securities, bonds, values or electronic payment instruments, by two legal provisions included in the Article 313 of the new Criminal Code. In addition to the previous version (2nd paragraph of Article 24 of the Law no. 365/2002), the legislator brings new legal charges, such as *receiving* and *transmitting forged values*. Meanwhile, if the perpetrator is, in the same time, the counterfeiter, the punishment proposed by the new Criminal Code will be the same as for the initial crime of forgery, and the two crimes will be regarded as in real concurrence (according to the 2nd paragraph). A new and interesting aspect has been brought by 3rd paragraph of Article 313 of the Criminal Code, which states that is a crime the act of putting a forged value again into circulation by the person who received the respective forged value and realized that was a fake, while the punishment stays the same as for the crime of forgery, with limits reduced to half.

As regarding the crime of *possession of equipments with the purpose of forging values* (Article 314), the 2nd paragraph refers exclusively to the situation of *possession of equipments with the purpose of forging electronic payment instruments*, and, compared to the previous version of the legal text (Article 25 of Law no.365/2002), there are two new actions incriminated, respectively *receiving* and *transmitting of equipments*. Another novelty is represented by the 3rd paragraph of Article 314, which states that there will be no punishment for the person who commits the crime, if followed by handing over the equipments to authorities or informing the authorities on the existence of these equipments, but before the authorities discover the crime by themselves and the forging actions occur. Worth noting that, despite the general tendency of reducing the imprisonment period, in this case the legislator has chosen to punish more severely the committing of this crime and increased the maximum limit of the prison time with 2 more years (from 5 years, in the previous version of the legal text).

Another crime, intensively highlighted by mass-media, given its various forms encountered in the judicial practice, is the *computer-related forgery*. The legislator kept the original form of the legal text (according to Article 48 of Law no.161/2003), but decreased the quantum of imprisonment period, as from 2 to 7 years (in pre previous version) to 1 to 5 years now.

This crime has been used and, most probably, will still be used, as a „universal legal solution", to resolve all those complex situations, for that, although requests existed, the legislator did not take concrete actions to implement proper legal provisions. For example, is the case of so-called *Phishing*, that method where the culprits (con artists) send to the victims well-designed email messages (masquerading as trustworthy entities or persons), with the purpose to mislead them to click on spoofed hyperlinks in order to access spoofed webpages controlled by the attackers, where the victims are lured to provide their personal or financial information, passwords or access codes. Generally, this kind of criminal action is called *social engineering*. Although this *Phishing* is committed by multiple material acts, it is currently legally solved by the prosecuting authorities only using the *computer-related forgery* crime. But, a deep analysis shows that, technically, only one action could be regarded as forgery, namely the forgery of the webpage used by culprits to illegally obtain data from the tricked victims. In fact, this is the sole action that has all the constituents to be regarded as the crime mentioned in Article 325 of the Criminal Code.

In what regards the communication of personal information on the spoofed webpage, there is no legal provision to incriminate the actions undertaken by the victims themselves, and the less to incriminate the activity of the culprits. On the other hand, tricking or misleading a person in order to acquire his personal or financial information are for sure criminal-type activities but not yet formalized in legal provisions and then, not subject to proper punishment (*nullum crimen sine lege*). A possible legal solution would have been the creation of a distinct article (with the name *ID theft* or *ID theft by means of electronic communications*) in this new Criminal Code, with the following text (as example): *(1) the obtaining of any personal data, where there is no consent from the entitled person, or by deception, and if electronic communications means have been used, is a crime and*

shall be punished with imprisonment from <x> months to <y> years. (2) The same punishment shall apply for the crime mentioned at paragraph (1) if committed by the use of electronic or eletromechanical devices designed to capture and store optic, magnetic or electric-representations of data.

In Title VII of the new Criminal Code a distinct Chapter (VI) was created with the name „Crimes against the safety and integrity of computer systems and data", which groups the majority crimes previously existing in Title III of Law no.161/2003.

Illegal access to a computer system (Article 360) is one of the most common offences in our judicial practice and still one of the most controversial in doctrine. In the new Criminal Code, the legislator preserved, almost identically, the previous legal provisions (paragraph 1 and paragraph 2 of Article 42 of Law no. 161/2003), while in paragraph 3 tried to reformulate the previous legal text but in a way that doesn't succeed to cover the real need for incrimination.

Although had the possibility, strictly in what regards the formulation of the legal text, the legislator did not modify the Romanian correct translation for the phrase „*illegal access TO a computer system*", in order to make it compliant to the text of the CoE Convention on Cybercrime. So, again the legislator choose to protect the access AT a computer system (in the Romanian language) instead of protecting the illegal access TO (meaning INSIDE) that computer system. As stated also in the Explanatory Report on the CoE Convention on Cybercrime, the importance of the access resides only in *entering the whole or any part of a computer system*, and not the access of the culprit in the vicinity of or around the computer system.

With the reference to the paragraph 3, although the legislator's intention was the creation of a legal text to fit the incriminating needs required by the prosecuting authorities, offering in the same time adequate safety measures against any abuse by law, the respective legal provision does not bring anything new, and, moreover, does not succeed to eliminate the various interpretations formulated in the course of time by practitioners and academics on the topic of „*infringing the security measures*".

In this context, a sensitive issue that did not find yet its solving, not even by reformulating paragraph 3, is still generated by the situation when the access to a computer system protected by security measures is committed by a perpetrator already knowing or being in possession of the needed access credentials (e.g. username, password, access code etc.). For example, the attacker who knows the username and the password associated to a login interface, uses them, and then get access to the respective computer system, but, technically, this is done without „forcing" or „eliminating" that security measure (login). Similarly, there could also be scenarios when the computer system has by default certain security measures in place but they has not been modified by the legitimate user, and thus may be known (or guessed) by any other person.

Under these hypothetical (but possible) conditions, an eventual criminal charging using Article 360 paragraph 3 of Criminal Code would be inadequate, at least from the following considerations: a) from the beginning, the legal text shows that we face an unauthorised intrusion in a computer system; b) the simple existence of certain procedures, devices or applications designed to restrict or forbid the access to that computer system cannot be regarded as an aggravating circumstance, taken into consideration that, anyway, the culprit finds himself already in a „illegal", „unauthorized" or „without right" status/situation with regard to that computer system. In the previous legal text (Article 42 paragraph 3 of Law no.161/2003), and according to the CoE Convention on Cybercrime, the Romanian legislator wanted to punish more severely the action of the person who, being already in a „illegal" relationship with a computer system, chooses to continue his criminal behaviour and performs certain technical operations to overwhelm, infringe or eliminate the security measures he confronts. In other words, the previous legal provisions highlighted more clearly, as aggravated circumstance, the „aggression"-type situation against the security measures and not just the simple operation on a computer system that has in place procedures, devices or applications by which the access to that computer is restricted or forbidden, as stated in the new Criminal Code.

As for the sanctioning regime, one could note the existence of the same limits of the imprisonment period (as in the previous legal text) – for the aggravated circumstance mentioned in paragraph 3 (3 years to 12 years), a decreasing of the punishment limits – for the circumstance mentioned in paragraph 2 (6 months to 5 years – now, to 2 years to 7 years - in the previous legal text), and also the introduction of the fine, as an alternative sanction for the circumstance provided in paragraph 1.

In what regards the crimes of *illegal interception of a non-public transmission of data* (Article 361), and *data interference - or altering computer data integrity* (Article 362), the legal texts in the new Criminal Code preserved almost identically the legal provision previously provided by Article 43 paragraphs 1 and 2, and Article 44 of the Law no.161/2003. In these cases, the only difference is in the sanctioning regime, with the decreasing of the imprisonment period from 2 to 7 years – in the previous versions, to 1 to 5 years in the new Criminal Code.

To the crime of *system interference – or disrupting the operation of computer systems* (Article 363) there are also no modifications compared to the previous version of the legal text (Article 45 of Law no.161/2003). In this case, too, the legislator only spotted a decreasing of the imprisonment period, as from 3 to 12 years – previously, to 2 to 7 years in the Criminal Code.

By the creation of a separate legal provision, namely Article 364, the legislator succeeded this time to split the crime of *unauthorized transfer of data* from the previous wrong context of *data interference* provided by Article 44 paragraph 2 and 3 of Law no. 161/2003, with respect to a technical reality – so that, by transferring computer data between systems or different storage media, no data shall be altered, suppressed, deleted or damaged in any way, loosing only the confidentiality of the information contained. Consistent with his trend, the legislator also modified for this crime the limits of the imprisonment period, as from 3 to 12 years – in the previous legal text, to 1 to 5 years in the new Criminal Code.

We need to emphasize that also this time, the legislator fails to provide a representation of the phrase „unauthorized", situation which may lead to difficulties in bringing a rigorous (truth-close) legal charge. In this scenario (unauthorized transfer of data), the phrase „unauthorized" or „illegal" may be applied only in conjunction with the culprit operations against the respective computer data, with the emphasize on the permission he has (or not) or the authorization he got (or not) to dispose of these data in the way he wants to. In what regards the interaction with the computer system the data is stored in, there shall be applicable the legal provisions of Article 360 – *illegal access to a computer system*. On the other hand, if the targeted data is also protected by other legal provisions, the criminal charge should be bound to a concurrence of crimes only if the culprit's action gathers all the constituents of such an offence.

The *unauthorized transfer of data* is an interesting crime, that could be easily and successfully used in those situations the prosecuting authorities or the courts of justice failed in the course of time to offer legal solutions for certain actions, such as, for example, the *Skimming method* meaning the illegal obtaining of identification data associated with credit cards, when the victims use these cards at ATMs, by mounting fake plastic ATM interfaces which embeds micro-controllers capable of reading the magnetic stripe of the cards) – in this case the credit cards acting as data storage means.

Another legal provision with large impact in the judicial practice nowadays is Article 365 – *misuse of devices and applications (or the illegal operations with devices and computer programs)*, which also preserves, with just a few modifications, the previous legal text provided by Article 46 of Law no. 161/2003. This provision continues to offer solutions to the various real life scenarios, when, under the guise of a legitimate trade, merchants (and not only) provide interested persons with electronic devices, computer programs and applications, passwords or access codes with the purpose to be used to further commit other computer-related offences against data and systems. From the text provided by paragraph 2 of Article 365 one could note an exaggeration of the legislator in using the phrase „without right". And, again, there is no explanation for the term „without right". Thus, the legal text states that shall be a crime the *possession, without right, of a device, a computer program,*

a password, an access code or any similar data, with the purpose of committing one of the crimes provided by Articles 360-364. In other words, is hard to imagine a situation when the possession of a certain application with the intent to commit an illegal access to a computer system is carried out „with right"! Also, compared to the previous legal text, the quantum of the imprisonment period has been decreased, as from 1 to 6 years (previously) to 6 months to 3 years or a fine (for the crime mentioned in paragraph 1), respectively 3 month to 2 years or a fine (for the crime mentioned in paragraph 2).

Placed in the general legal context of Title VIII – Crimes affecting the relations of social life, the Article 374 gathers all the criminal actions committed by using child pornography materials. Compared to the previous version of the legal text (Article 51 of Law no.161/2003), there are new incriminations, such as *storage, promotion, exposure, distribution (sharing)* or *accessing* (of child pornography materials). Other changes aimed at: broadly incriminating the *production* of child pornography materials – whereas in the previous version of the legal text the same action was committed only *for the purpose of sharing*, putting the *possession* in conjunction with a certain purpose, such as: the *exposure* or the *distribution* of pornographic materials with children (compared with Law no.161/2003 which simply incriminates the *possession without right*). On the other hand, one could note that the phrase „without right" has been „moved" now just for the context of *accessing child pornography materials*, the legislator assessing that this action is the only one that could be carried out, in certain conditions, even „with right".

In what regards the sanctions, the legislator eliminated the complementary punishment of restricting certain rights to the defendant, and maintained the general trend of decreasing the imprisonment period limits, as from 3 to 12 years – in the previous legal text, to 2 to 7 years (for paragraph 2), respectively 3 months to 3 years or a fine (for paragraph 3).

Electronic vote interference (or electronic vote-related fraud), provided by Article 388 has no previous correspondent, being only mentioned as a possibility in the Government Emergency Ordinance no.93/2003 on casting the vote by electronic means to the national referendum for the revision of the Constitution. Formalized in a single legal provision, the crime consists of the printing and using false access data, illegal access to the electronic vote system, and forgery by any means of the digital ballots. As a general observation, these actions could be committed in ideal concurrence with other computer-related crimes, such as the *access to a computer system* or *computer-related forgery*. There have also been reduced the limits of the imprisonment period, as from 2 to 7 years (previously), to 1 to 5 years in the new Criminal Code.

The criminal context with regard to the electronic vote has been completed with Article 391 – *forging the electoral documents and records*, a crime previously comprised, by pieces, in Articles 60 and 61 of Law no.35/2008 – the electoral law. The text modifications are insignificant, and the quantum of the imprisonment period has been preserved in the same limits. Given the digital environment where such crimes occur, this offence might be subject of ideal or real concurrence with other computer-related crimes, such as: *data interference, system interference* or *computer-related forgery*.

Conclusions

The new Criminal Code answers in a proper way the challenges posed by cyberspace, providing useful legal tools to practitioners in combatting a wide range of criminal behaviour against computer data, systems and telecommunications.

Overall, worth to be underlined that the modifications brought to the previous Romanian legislation are relevant in relation to the actual need of incrimination resulted from the analysis of the local judicial practice, while the new aspects essentially contribute to the creation of a modern legal framework, fully able to protect in the future those social values that will not wait to emerge from the virtual interaction between individuals and a information technology in great expansion.