PAPER:

THE DIGITAL ECONOMY – WHERE IS THE EVIDENCE? THEORETICAL AND PRACTICAL PROBLEMS IN UNDERSTANDING DIGITAL EVIDENCE IN ROMANIA

By **Bogdan Manolea**

Introduction

The developments in the past decade in Romania in respect of Information Technology have changed the way many businesses manage and perform their activities. Not only has the digital economy flourished, reaching approximately 120 million in 2007,[1] but the general trend of using computers in the personal daily experience or in work-related activities has become a reality. According to the latest figures available from the National Authority on Communications and Information Technology, approximately 27 per cent of Romanians have access to the internet, and 10 per cent to a broadband connection.[2] But the figures sometimes hide part of the reality: a major divide between rural and urban areas or between the younger and older generation.

Legislation and implementation

During the accession process to the European Union, Romania implemented the EU Directives in the field of e-commerce (Lege nr. 365 din 7 iunie 2002 privind comertul electronic) and on electronic signatures (Lege nr. 455 din 18 iulie 2001 privind semnatura electronica).[3] However, the Directives have only been transposed, without too much consideration for an overall policy, general scope or connection with other existing normative acts. Although the legislation has been in place for some years, the interpretation and understanding of the law is not one of the strong points of the judiciary, and this is the case for all the legislation relating to information technology matters. Moreover, the creation of competent authorities in these fields has not been high on the list of priorities by the government. In 2007 the responsibility for e-commerce and e-signatures passed from the Ministry of Communications and Information Technology to an independent authority, the National Authority for Communications and Information Technology.[4] Within this general framework, electronic evidence has not and is not considered as one of the priorities for the digital economy, even though more evidence in a digital format is produced every day. Without a requirement from the EU requiring special provisions in respect of electronic evidence, the Romanian Government has not exhibited an interest in this topic.[5]

Only the practical problems, in relation to internet

[1] *Anca Arsene, 'Comertul electronic online, o piata de 120 de milioane de euro anul viitor,' Ziarul Financiar, 28 September 2006, available at http://www.zf.ro/articol_96468/comertul_electronic_online__o_piata_de_120_de_milioane_de_euro_anul_viitor.html.*

[2] *Details available from National Authority on Communications and Information Technology, http://www.anrcti.ro.*

[3] *Law on e-commerce no 365/2002 (for unofficial translations, see http://www.legi-internet.ro/index.php?id=237&L=2) and Law on e-signature no 455/2001 (for unofficial translations see http://www.legi-internet.ro/index.php/Law_on_the_Electronic_Signatur/71/0/?&L=2).*

[4] *Change made according with the Emergency Ordinance of the Government no 134 regarding the setting up of the National Authority for Communications and Information Technology (ANRCTI) (Ordonanta de Urgenta nr.134 din 21 decembrie 2006 privind înfiintarea Autoritatii Nationale pentru Reglementare în Comunicatii si Tehnologia Informatiei).*

[5] *However, see Dana Irina Cojocarasu and Oana Irina Ignat, 'Romania', in Stephen Mason, editor, International Electronic Evidence (British Institute of International and Comparative Law, 2008).*

fraud and phishing activities, have caused law enforcement authorities to respond – after some pressure from those foreign counterparts directly affected by these illegal activities.[6] It is for this reason that the inclusion and use of digital evidence in court has been more effective in criminal proceedings, rather than in civil proceedings. Other efforts in designating special law enforcement authorities to deal with internet fraud and phishing, and educating officers in becoming cybercrime specialists, have been instrumental in reducing the number of computer crime cases in Romania, but this has proven to be just the beginning. The phishing cases that were targeting only foreign internet users and financial institutions have expanded, and in the past year there has been an increase in phishing attacks targeted against Romanian banks.[7] The early fraud internet-related cases are comparatively modest in comparison to the new organized structures that are involved in internet crime today, with the use of recruits from more than one or two countries to make matters more complicated.

Digital evidence in civil cases

Digital evidence is not present to a high degree in civil proceedings. Even when it is obvious that it is just a matter of time when evidence in a digital format will become the rule, rather than the exception, it is difficult to understand the lack of preparation and education for judges and lawyers. At the time of writing, there is no obligatory or voluntary course on IT law at the Institute of Magistracy, and the current IT courses focus only on how to use a computer and not to understand the kind of evidence to be found in an IT system. This situation is compounded by the fact that the law faculties in universities do not have regular IT law courses, with some minor exceptions, but rather prefer to support courses on legal informatics. In practice, this means that the legal experts involved with a case regarding digital evidence need either to try to understand the computer-related aspects or look for technical expertise in order to better manage the case.

To date, there is a tendency to assimilate digital evidence with the old civil procedure institutions.[8] Therefore in some civil proceedings, electronic mail has been accepted by the courts as a valid form of evidence where the other party does not contest the correspondence in question.[9] Also, evidence of the content of a web page has been assimilated with the 'beginning of the documentary evidence'[10] by means of the 'Print Screen' instructions, and can be accepted by the courts as an item real evidence, but only if included with other evidence. In order to ensure the evidence has a higher value, the 'Print Screen' process can be conducted before a public notary or a bailiff,[11] and in so doing, a precise date is also obtained for the content of the print screen process.

In particular, it is necessary to emphasise the problem with submitting to the court a fact or item of documentary evidence that is publicly available on the internet. It is possible that the party could just indicate the URL where the evidence can be found or, also, could try to present in court, with the help of a computer and a wireless internet connection, the document available on the internet.[12]

Problems with experts

Besides the elements mentioned above, the parties or the judge will usually request a technical report by a digital evidence specialist,[13] in order to clarify the technical aspects or to bring more evidence that is available in the computer system in order to enable the judge to more fully understand the evidence. But here the situation becomes complicated. In accordance with Romanian law, the judge must select one or three experts in the relevant field to undertake the necessary work.[14] The experts are selected from a special list that exists in every tribunal.[15] Requesting a report from an expert is considered a rather long and complicated procedure (for instance, in the experience of the author, conducting the enquiry and the drafting of the report could take at least six months from the moment the report is requested, depending on the complexity of the case). In addition, the parties or the judge can demand, after the report has been filed with the case, a supplementary or a further report by another expert that could lengthen the time it takes a judge to reach a decision.[16]

In the experience of the author, the current list of

[6] *For example, see Georgeta Ghidovat, ' Politistii si procurorii, scoliti de eBay sa-i faca fata hackerului Vladutz' (Policemen and Prosecutors trained by eBay to react to Hacker Vladutz), Cotidianul, 14 May 2008' available at http://www.cotidianul.ro/politistii_si_procurorii_scoliti_de_ebay_sa_i_faca_fata_hackerului_vladutz_video-45832.html.*

[7] *For example, see Radu Rizea, ' Phishing attack against Piraeus Bank clients', Hotnews, 25 June 2008 available at http://english.hotnews.ro/stiri-business-3354213-phishing-attack-against-piraeus-bank-clients.htm.*

[8] *Codul de procedură civilă (Civil Procedure Code), available at http://www.dreptonline.ro/legislatie/codul_procedura_civila_consolidat.php and http://legal.dntis.ro/cpcivil/index-cpc.html.*

[9] *Articles 172 and 177, Civil Procedure Code.*

[10] *Article 1197, Civil Code.*

[11] *In Romanian: executor judecatoresc, legal institution similar with the French Hussier de Justice, for more information see the webpage of the National Union of Bailiffs at http://www.executori.ro/.*

[12] *This is a possible interpretation in accordance with the provisions of Articles 215-217, Civil Procedure Code.*

[13] *Experts in civil proceedings are regulated by Articles 201-214, Civil Procedure Code.*

[14] *Article 210(1), Civil Procedure Code.*

[15] *There are 42 Tribunals in Romania, established on territorial grounds and competence. The list is available on the Ministry of Justice website, http://portal.just.ro/InstanteLista.aspx.*

[16] *Article 212, Civil Procedure Code.*

experts[17] does not contain any digital evidence specialists or a similar definition. This does not mean that digital evidence specialists are not on the list, but usually the list contains less than two persons per Tribunal.[18] In Bucharest or Timisoara[19] there are only between two and three experts that might have sufficient expertise, and they are all from the old lists of experts. It can be inferred from this that it is almost impossible to find a digital evidence specialist on the list of experts with sufficient knowledge to provide an adequate report to the court.

Another problem with the lack of digital evidence specialists, is that the judge needs to understand at least the essential part of a case, and the court is required to establish the reason for employing the expert and the questions that the digital evidence specialist is required to answer. The lack of even a basic knowledge in computers often creates real problems in addressing relevant questions to the expert. Sometimes the judge will accept the questions raised by the lawyers that represent the parties. Unfortunately, lawyers frequently fail to consult with any qualified digital evidence specialists, so the expert may be given a list of questions to which they cannot answer from a pure technical point of view. The lack of relevant experts on the lists of the Tribunals could be resolved by accepting other specialists by the court, taking into account that the IT security business is well developed in Romania. But, unfortunately, the courts are generally reluctant to use this exceptional procedure. It is difficult to understand why the judges are reluctant, since the provisions of article 201 paragraph 3 of the Civil Procedure Code permits the court or the parties to ask any relevant specialist to undertake a report, if there are no experts on the official list.

Following Romania's entry into the European Union, another possibility is that the legal framework on expertise can be modified, allowing experts from other EU member countries to be accepted in a Romanian court, if they are accepted according with the rules of the country of origin.[20]

The principle of the free assessment of the evidence, as in the case of other forms of evidence, allows a judge to decide on the importance of the need for an expert, depending on the facts of each case and taking into account the other elements presented in the case.[21] Whatever decision is made, the judge must explain in their decision the reason why they took into consideration the report and evidence of the expert or not. In reality, in the majority of cases, the court accepts the opinion of the expert and tries to use that information in order to select the applicable legal text.

In the current situation explained above, it is not surprising that where litigants realise that most of their case is based on digital evidence, they are reluctant to initiate litigation in civil or commercial cases, and they try to solve the problem or just ignore it. Unfortunately, there are no alternative dispute resolution methods developed to deal with specific IT law cases or e-commerce cases.

Digital evidence in criminal proceedings

As has been explained above, the existence of many complaints relating to internet fraud and phishing cases initiated from Romania caused a much better response in tackling this new phenomenon and in presenting digital evidence in criminal proceedings. It is estimated that 75-80 per cent of the computer-related cases investigated by the Romanian police deal with phishing cases. Today, there are specialized police forces in Bucharest and other major cities in Romania dealing with cybercrime cases. Also, prosecutors have received special training against organized crime,[22] which means they are in a better position to investigate crimes and prepare the case for court proceedings. At the same time, the police include digital evidence specialists as well as in the National Institute of Forensics and the Romanian Intelligence Service.

From a substantial criminal law point of view, Romania has implemented the Cybercrime Convention[23] in its national legislation.[24] Therefore all the computer crimes have been defined, with little modification. The

[17] *The list is publicly available on the Ministry of Justice website http://www.just.ro/MeniuStanga/Listapersoanelorautorizate/Expertijudiciari/tabid/160/Default.aspx.*

[18] *A search of the list using the keyword 'computers' gave 10 results of judicial experts.*

[19] *Bucharest and Timisoara are illustrated because of the author's knowledge regarding the number of local experts, and because there are two of the top three cities in Romania.*

[20] *In accordance with the changes made through Law no 247/2005 (Legea 247/2005 privind reforma în domeniile proprietatii si justitiei, precum si unele masuri adiacente) published in the Official Monitor no 653 on 22.7.2005, and Emergency Ordinance 109/2007 (Ordonanta de urgenta nr. 109/2007 pentru modificarea si completarea Legii nr. 200/2004 privind recunoasterea diplomelor si calificarilor profesionale pentru profesiile reglementate din Romania), published in the Official Monitor no 706 on 18.10.2007.*

[21] *Viorel Mihai Ciobanu, Theoretical and practical treaty of civil procedure, Volume II, (1997, Ed National), 212.*

[22] *Also known as DIICOT- Division of Investigation Organized Crimes and Terrorism Crimes – more details regarding its attributions are available on the Public Ministry website at http://www.mpublic.ro/regulament_PICCJ.htm#diicot.*

[23] *Council of Europe - ETS No. 185 - Convention on Cybercrime, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.*

[24] *Law 161/2003 – Title III, Preventing and Combating Cybercrime (Legea 161 din 19/04/2003 privind unele masuri pentru asigurarea transparentei în exercitarea demnitatilor publice, a functiilor publice si in mediul de afaceri, prevenirea si sanctionarea coruptiei - TITLUL III Prevenirea ºs combaterea criminalitãtii informatice). An unofficial English translation is available at http://www.legi-internet.ro/index.php/Romanian_Cybercrime_Law/84/o/?&L=2.*

same law that implemented the cybercrime convention has specific procedural penal law provisions[25] regarding the preservation of stored computer data, the search and seizure of stored computer data, which can be undertaken by a prosecutor or a judge, and the real-time collection of traffic and content of computer data, that can only be demanded by a judge.[26]

In cases of emergency, when it is possible that evidence can be altered quickly – which tends to be the rule in the IT domain – the Romanian Penal Procedure Code gives prosecutors the power to ask for a Technical Observation,[27] which is undertaken by specialists within the police forces or the office of the prosecutor. The result comprises the Technical Observation report,[28] and this is part of the evidence presented by the prosecutor in their case. Since special IT forensic expert groups have been created in Bucharest and other major cities within the police forces, they are the ones usually responsible for the Technical Observation reports for computer systems, having undertaken specialized training and having access to special IT forensic software. For more complicated cases that involve computing devices or parts of computer devices that have been made by individuals and that might be used for committing computer crimes, these forms of evidence are sent to be examined under the Technical Observation procedure to the Romanian Intelligence Service or the National Forensic Institute.

The investigation of criminal matters, although much better organized in relation to the gathering and presenting of digital evidence, does have some problems. The reality indicates that digital evidence is very often used in order to determine other forms of evidence that are much easier for a judge to understand: for example, the prosecutors try to obtain confessions from the accused or their accomplices. It is not uncommon that some judges do not understand the case as such, which means most of the time they accept the prosecutor's arguments in the case. This creates problems from the point of view of the defendant, especially in order to create and support a valid and acceptable defence, since they lack access to the digital evidence specialists in order to contradict the prosecutors allegations. Because of the issue of the digital evidence specialists,[29] there is, in essence, a similar problem in criminal proceedings as there exists in civil proceedings.

In criminal matters, the law does not permit the nomination of other experts where the names of IT experts already exist on the list, with the exception of 'special circumstances'.[30] However, the digital world is even more specialized than ever, and 'special circumstances' may appear in every case dealing with a computer system. Therefore, in order not to complicate some cases too much, there have been situations when a judge has decided to accept the opinions of the Technical Observation Report and to refuse to appoint an independent expert, because it will take too much time, especially if it involves a foreign server. But with the way the internet is used now, this might soon become the rule in investigating on-line cybercrime cases

In accordance with the procedure, the parties and the judge will decide on a list of questions for the expert, and the expert will be required to present a written report. The parties each have the right to nominate a recommended expert that will take part in the expertise.[31] Also, if the expert fails to provide the required answers, the judge or the parties may ask supplementary questions of the expert or appoint another expert. As with the presentation of the expert's evidence and report in civil proceedings, the judge can decide on the importance of the expert report and evidence in accordance with the principle of the free assessment of the evidence, depending on each case and in corroboration with the other elements presented in the case.[32]

However, even when the expert provides the required answers, due to the complexity and high level of technical issues in an internet fraud case, for example, it is very often not easy for a judge with little information and understanding on how the internet works to decide exactly what crime has been committed and what the social danger is in the specific case in order to ensure the punishment fits the crime. In the opinion of the author, the present decisions of Romanian judges in the phishing cases do not indicate the full extent of the difference in degree of criminal acts, and either consider the criminals as small IT geniuses that deserve a second chance to work in IT security, or dangerous 'hackers'

[25] *Articles 54-59 from Law 161/2003.*
[26] *For a detailed overview of the Romanian cybercrime laws and its procedural dispositions, see Maxim Dobrinoiu, Informatic Crimes, (Ed Ch Beck, 2006).*
[27] *Ion Neagu, Treaty-Penal Procedure Law, (Global Lex, 2002), 379.*
[28] *See the details in Articles 112-115, Penal Procedure Code.*
[29] *The legal provisions regarding the role and attributions of experts in criminal proceedings is regulated by Articles 116-125, Penal Procedure Code.*
[30] *Ion Neagu, Treaty-Penal Procedure Law, (Global Lex, 2002), 386.*
[31] *Following the Constitutional Court Decision no 143 from 5.10.1999 published in the Official Monitor no. 585 on 30.11.1999 (Decizia Curtii Constututionale nr.143 din 5 octombrie 1999 referitoare la exceptia de neconstitutionalitate a dispozitiilor art. 120 alin. 5 din Codul de procedura penala).*
[32] *Ion Neagu, Treaty-Penal Procedure Law, (Global Lex, 2002), 389.*

that should spend a long time in prison.[33]

Some conclusions

At the time of writing, generally speaking digital evidence is not well understood by lawyers, judges and many experts in Romania. In order to change this position, it is necessary to accelerate the education of lawyers, judges and experts in order to better understand digital evidence. Also, it is necessary to consider relaxing the rules relating to the admission of experts into legal proceedings. All those people that can be included in the legal domain need to better understand that computer activities and digital evidence are in a state of continuous development, and it is therefore necessary to change procedural rules needs in order to have a functioning and reliable justice system in the twenty first century.

Bogdan Manolea is the Executive Director, Association for Technology and Internet - APTI (Romania). Bogdan has a legal background with experience in the Law and IT & C. He runs the only Romanian web site dedicated to IT law, where he also regularly blogs about ITC & legal issues.

http://www.legi-internet.ro

[33] *This problem is debated in the author's blog: Hei, Vladutz, Vladutz, 18 April 2008 at http://legi-internet.ro/blogs/index.php?title=mai_vladutz_vladutz&more=1&c=1&tb=1&pb=1.*

